Corso di Algebra III
2. Appunti di Algebra Commutativa

Avvertenza

Queste note sono in buona parte un estratto dal libro di testo,

A.M. - M. Atiyah, I. MacDonald, *Introduction to Commutative Algebra*,

e il loro scopo è quello di aiutarne la lettura e lo studio. Con questo intento abbiamo pensato potesse risultare utile

1. sviluppare con con maggiore dettaglio alcuni esempi presi dal testo, ed aggiungerne altri che ci parevano interessanti se non istruttivi;

2. fornire la soluzione di alcuni (per il momento non tantissimi) esercizi.

Gli esercizi tratti dal testo sono richiamati tra parentesi mediante due numeri: il primo indica il capitolo del libro in cui compare l'esercizio, il secondo il suo numero progressivo. Ad esempio, ex. 3.11 indica l'esercizio n. 11 del capitolo 3 in A.M. Va da sé che chi studia cercherà seriamente di risolvere per proprio conto ciascun esercizio prima di confrontare la soluzione qui fornita.

1 Ideali e radicali

[questa parte è associata al capitolo 1 di A.M.]

Come nel libro A.M., per tutte queste note con il termine "anello" si intende un *anello commutativo con identità* 1_A (che spesso denoteremo solo con 1).

Una differenza rispetto alle convenzioni stipulate nel corso di Algebra I riguarda il non escludere che in un anello A si abbia $1 = 0$; in tal caso, A è necessariamente costituito da un unico elemento, $A = \{0\}$ e si chiama *anello nullo*. Questo consente di parlare di anello anche per il quoziente A/A, di un anello modulo l'ideale improprio. Il prezzo che si paga è che in molti enunciati sarà un caso da escludere in partenza; volendo far ciò ricorreremo alla formula "sia A un anello non-nullo", oppure "sia $A \neq (0)$ un anello".

Questa sezione introduttiva è composta da richiami di concetti e risultati basilari, riguardanti gli anelli, già studiati nel corso di Algebra I, e da alcune altre osservazioni di carattere fondamentale (Lemma di Zorn e ideali massimali) o di natura più tecnica, per le quali, non essendo state trattate in precedenza, si forniscono le dimostrazioni.
Non tutto ciò che occorre aver presente della teoria degli anelli e dei campi, studiato nei corsi di Algebra I e II, sarà esplicitamente richiamato: è il caso, ad esempio, di molte definizioni di base, come quelle di ideale, di quoziente, e di omomorfismo (isomorfismo), di prodotto diretto, così come dei concetti e teoremi connessi agli omomorfismi stessi: nucleo, immagini e immagini inverse, il Teorema di omomorfismo e l'importantissimo Teorema di Corrispondenza: tutte cose per le quali si rimanda direttamente agli appunti dei corsi di Algebra passati.
Un'ultima avvertenza: negli enunciati e nelle definizioni anche di questa sezione si assume - come concordato all'inizio - che gli anelli in gioco siano commutativi; questo anche quando tale ipotesi non è strettamente necessaria. Si tratta tuttavia di risultati già noti a chi legge, che non avrà difficoltà a ricordare (o riprovare) se e in quali casi la commutatività sia un'ipotesi non eliminabile.

1.1 Ideali

Se I, J sono ideali dell'anello A, allora $I \cap J$ è un ideale. Più in generale, dato un insieme non vuoto Σ di ideali di A, l'intersezione

$$\bigcap_{I \in \Sigma} I$$

è un ideale di A.
Se X è un sottoinsieme di A, e Σ l'insieme di tutti gli ideali contenenti X (non è vuoto dato che $A \in \Sigma$) allora $\bigcap_{I \in \Sigma} I$ è il minimo ideale di A che contiene X: è l'ideale *generato*

da X e si denota con (X). Se $X = \{x_1, \dots x_k\}$, si scrive $(X) = (x_1, \dots, x_k)$; si prova facilmente che, in tal caso,

$$(X) = \{a_1x_1 + \cdots a_nx_n \mid n \geq 1,\ x_i \in X,\ a_i \in A\}. \tag{1}$$

In particolare, se x è un elemento dell'anello A l'ideale

$$(x) = \{ax \mid a \in A\} = Ax$$

si dice *ideale principale* generato da x (e un ideale I si dice principale se esiste $x \in A$ tale che $I = (x)$). L'ideale nullo (0) e l'intero anello $A = (1)$ sono ideali principali.

Un elemento a di un anello A si dice *invertibile* (o *unità*) se esiste $b \in A$ tale che $ab = 1$; in tal caso b è univocamente determinato, si denota con a^{-1} e si chiama *inverso* (moltiplicativo) di a. Il prodotto di elementi invertibili è invertibile; ciò comporta che l'insieme degli elementi invertibili, che denoteremo con $U(A)$, è un gruppo rispetto al prodotto in A.

Un *campo* è un anello non-nullo in cui ogni elemento $\neq 0$ è invertibile.

Proposizione 1. *Sia A un anello non nullo.*

(1) *Per ogni $x \in A$, x è invertibile se e solo se $(x) = A$.*

(2) *A è un campo se e solo se (0) è il solo ideale proprio di A.*

(3) *A è un campo se e solo se ogni omomorfismo d'anelli $A \to B$, con $B \neq 0$, è iniettivo.*

Un elemento a di un anello A si dice *divisore dello zero* se $a \neq 0$ ed esiste $b \in A$, $b \neq 0$, tale che $ab = 0$. Un anello privo di divisori dello zero si chiama *dominio d'integrità*.

Ogni dominio d'integrità A si estende al suo e univocamente determinato *campo delle frazioni*, secondo una procedura che sarà estesa nella sezione 4.

Un *dominio a ideali principali* (PID) è un dominio d'integrità in cui ogni ideale è principale. Esempi banali di PID sono i campi; esempi fondamentali sono l'anello dei numeri interi $\mathbb{Z}$ e gli anelli di polinomi $\mathbb{K}[x]$ in un'unica indeterminata a coefficienti su un campo $\mathbb{K}$. I domini d'integrità $\mathbb{Z}[x]$ e $\mathbb{K}[x_1, \dots, x_n]$ (con $n \geq 2$) non sono a ideali principali (sono tuttavia a fattorizzazione unica - vedi dispense di Algebra I).

Definizione. Sia I un ideale dell'anello A.

(1) I è un ideale *primo* se è proprio e, per ogni $x, y \in A$:

$$xy \in I \ \Rightarrow\ x \in I \text{ o } y \in I.$$

(2) I è un ideale *massimale* se è proprio e per ogni ideale J di A:

$$I \subseteq J \;\Rightarrow\; J = I \text{ oppure } J = A.$$

Ideali primi e ideali massimali si possono caratterizzare in termini di proprietà dei corrispondenti quozienti.

Proposizione 2. *Sia I un ideale proprio dell'anello A.*

(1) *I è primo se e solo se A/I è un dominio di integrità.*

(2) *I è massimale se e solo se A/I è un campo.*

(3) *Se I è massimale allora I è primo.*

1.2 Operazioni con gli ideali

Somme. Se I e I sono ideali dell'anello A allora

$$I + J := \{x + y \mid x \in I,\ y \in J\}$$

è un ideale di A. Dall'identità (1) segue che $I + J$ è il più piccolo ideale che contiene l'unione $I \cup J$; quindi, ad esempio, se $X = \{x_1, \dots x_k\}$ è un sottoinsieme finito dell'anello A allora

$$(x_1, \dots, x_k) = (x_1) + \dots + (x_n) = Ax_1 + \dots + Ax_k$$

Il concetto si estende ad una famiglia infinita Σ di ideali di A; in tal caso, la *somma* degli ideali di Σ è l'ideale generato dalla loro unione, e risulta l'insieme costituito da tutte le somme di un numero *finito* di elementi appartenenti a qualche ideale I della famiglia:

$$\sum_{I \in \Sigma} I = \Big\{ x_1 + \cdots + x_n \mid n \geq 1,\ x_1, \dots, x_n \in \bigcup_{I \in \Sigma} I \Big\}.$$

Due ideali I e J si dicono *coprimi* se sono propri e $I + J = A$.

Prodotti. Se I e I sono ideali dell'anello A, con la scrittura IJ si intende l'ideale di A generato da tutti i prodotti xy, con $x \in I$ e $y \in J$; quindi,

$$IJ = \sum_{x \in I} xJ.$$

Chiaramente,

$$IJ \subseteq I \cap J. \tag{2}$$

La definizione si estende in modo naturale: se $I_1, \dots, I_n$ sono ideali di A, si pone

$$I_1 I_2 \cdots I_n = \big(\{ x_1 x_2 \cdots x_n \mid x_i \in I_i,\ i = 1, \dots, n \} \big)$$

(si verifica facilmente che $I_1 I_2 \cdots I_n = I_1(I_2 \cdots I_n)$, etc.). Se $I_1 = I_2 = \ldots = I_n = I$ si scrive

$$I_1 I_2 \cdots I_n = I^n.$$

ESEMPIO 1. Nell'anello di polinomi $A = \mathbb{K}[x_1, \ldots, x_n]$ (dove $\mathbb{K}$ è un campo e $x_1, \ldots, x_n$ indeterminate indipendenti) sia $J = (x_1, \ldots, x_n)$; allora per $n \geq 1$, J^n è l'insieme di tutti i polinomi privi di termini di grado strettamente minore di n.

Siano I, J, L ideali di un anello A; le seguenti identità sono facilmente verificabili:

(1) (proprietà distributiva) $I(J + L) = IJ + IL$;

(2) (legge modulare) se $I \supseteq J$ allora $I \cap (J + L) = J + (I \cap L)$;

(3) $(I + J)(I \cap J) \subseteq IJ$.

In generale, in $IJ \subseteq I \cap J$ non vale l'uguaglianza; ad esempio, si considerino in $\mathbb{Z}$ gli ideali $I = 6\mathbb{Z}$ e $J = 10\mathbb{Z}$, allora $I \cap J = 30\mathbb{Z}$ mentre $IJ = 60\mathbb{Z}$. Si ha tuttavia la seguente utile proprietà.

Lemma 3. *Sia $n \geq 2$ e siano $I_1, I_2, \ldots, I_n$ ideali a due a due coprimi di un anello A; allora*

$$I_1 \cap \ldots \cap I_n = I_1 \cdots I_n.$$

Dimostrazione. Induzione su n. Se $n = 2$, $1 = x + y$ con $x \in I_1$ e $y \in I_2$; sia $u \in I_1 \cap I_2$, allora $u = u1 = ux + uy \in I_1 I_2$,. Quindi $I_1 \cap I_2 \subseteq I_1 I_2$ e, poiché l'inclusione inversa è ovvia, si ha l'uguaglianza $I_1 \cap I_2 = I_1 I_2$.
Sia $n \geq 3$. e scriviamo $J = I_2 \cap \ldots \cap I_n$; allora, per ipotesi induttiva, $J = I_2 \cdots I_n$. Poiché I_1 è coprimo con gli altri I_i, per ogni $2 \leq i \leq n$ esistono $x_i \in I_1$ e $y_i \in I_i$ tali che $x_i + y_i = 1$; ma allora per un opportuno $x \in I_1$,

$$1 - x = (1 - x_2)(1 - x_3) \cdots (1 - x_n) = y_2 y_3 \cdots y_n \in J,$$

e quindi $1 = x + y_2 \cdots y_n \in I_1 + J$. Dunque I_1 e J sono coprimi; pertanto

$$I_1 \cap I_2 \cap \ldots \cap I_n = I_1 \cap J = I_1 J = I_1 I_2 \cdots I_n,$$

come si voleva. □

Esercizio 1. [Teorema Cinese dei Resti] Siano $I_1, I_2, \ldots, I_n$ ideali a due a due coprimi di un anello A, e sia $J = I_1 I_2 \cdots I_n$; si provi che

$$\frac{A}{J} \simeq \frac{A}{I_1} \times \frac{A}{I_2} \times \cdots \times \frac{A}{I_n}.$$

L'unione di due ideali è un ideale se e solo se uno dei due ideali contiene l'altro. Per unioni di ideali primi vale una proprietà ancor più forte (e come vedremo piuttosto utile): un ideale che sia contenuto nell'unione di un numero finito di ideali primi è già contenuto in uno di essi.

Lemma 4. [Prop. 1.11 in A.M.] *Siano $Q, P_1, \dots P_n$ ideali di un anello A,*

(1) *Se $P_1, \dots P_n$ sono ideali primi e $Q \subseteq \bigcup_{i=1}^n P_i$, allora $Q \subseteq P_i$ per qualche $1 \leq i \leq n$.*

(2) *Se Q è un ideale primo e $Q \supseteq P_1 P_2 \cdots P_n$ (in particolare se $Q \supseteq \bigcap_{i=1}^n P_i$) allora $Q \supseteq P_i$ per qualche $1 \leq i \leq n$. Quindi, se i P_i sono ideali massimali, $Q = P_i$ per qualche i.*

Dimostrazione. (1) Per induzione su n. Dato che il caso $n = 1$ è l'ipotesi, sia $n \geq 2$. Se, per qualche $1 \leq i \leq n$, si ha $Q \subseteq \bigcup_{j \neq i} P_j$, allora l'affermazione segue dall'ipotesi induttiva. Possiamo quindi assumere che per ogni $1 \leq i \leq n$ esista $x_i \in Q \setminus \bigcup_{j \neq i} P_j$; osserviamo che allora per ogni $1 \leq i \leq n$, $\prod_{j \neq i} x_j \notin P_i$, dato che P_i è un ideale primo. Dunque, se

$$y = x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \ldots + x_1 x_2 \cdots x_{n-1},$$

allora $y \in Q$, ma $y \notin P_i$ per ogni $1 \leq i \leq n$, che è una contraddizione.

(2) Supponiamo $P_i \not\subseteq Q$ per ogni $1 \leq i \leq n$. Allora, per ogni tale indice i, esiste un elemento $x_i \in P_i \setminus Q$. Ma allora $x_1 x_2 \cdots x_n \in P_1 \cdots P_n \subseteq Q$ e, poiché Q è primo, si ha la contraddizione $x_i \in Q$ per qualche $1 \leq i \leq n$. □

1.3 Lemma di Zorn, ideali massimali, anelli locali

Definizione. Un insieme parzialmente ordinato, o *poset*, $(\Sigma, \leq)$ si dice *induttivo* se ogni suo sottoinsieme totalmente ordinato (*catena*) ammette un maggiorante.

Lemma di Zorn. Ogni insieme parzialmente ordinato induttivo non vuoto ammette elementi massimali.

Molte applicazioni del lemma di Zorn in teoria degli anelli (come la fondamentale Proposizione 6 a seguire) si basano su un'osservazione piuttosto elementare, la cui dimostrazione, abbastanza ovvia, dipende a sua volta dal fatto che un ideale I di un anello A è proprio se e solo se $1 \notin I$.

Lemma 5. *Sia $\mathcal{I}$ una famiglia di ideali* propri *dell'anello A (non necessariamente commutativo). Se $\mathcal{I}$ è totalmente ordinata per inclusione allora $\bigcup_{I \in \mathcal{I}} I$ è un ideale proprio di A.*

Proposizione 6. (i) *Sia A un anello (non necessariamente commutativo) e sia I un ideale proprio di A; allora esiste un ideale massimale M di A, con $I \subseteq M$.*

(ii) *Se A è commutativo e $a \in A$ è un elemento non invertibile, allora esiste un ideale massimale di A che contiene a.*

Dimostrazione. Sia Σ l'insieme di tutti gli ideali propri di A che contengono I. $\Sigma \neq \emptyset$, dato che $I \in \Sigma$, e Σ, ordinato per inclusione, è un poset induttivo per il Lemma precedente. Per il Lemma di Zorn, Σ ammette un elemento massimale M, che chiaramente è un ideale massimale di A e, per definizione, contiene I.
La seconda parte si deduce dalla prima tenendo conto che, se A è commutativo e $a \in A \setminus U(A)$, allora l'ideale generato da a, $(a) = Aa$, è un ideale proprio di A. □

Quindi, in un anello commutativo un elemento è invertibile se e solo se non è contenuto in alcun ideale massimale.

Definizione. Un anello A con un unico ideale massimale si dice *anello locale*. In tal caso, se M è l'unico ideale massimale di A, il campo A/M è detto *campo residuo* dell'anello locale A.

Proposizione 7. 1) *Sia A un anello locale e sia M il suo unico ideale massimale; allora $M = A \setminus U(A)$.*

2) *Sia M un ideale proprio dell'anello A, tale che $A \setminus M \subseteq U(A)$, allora A è un anello locale e M è il suo unico ideale massimale.*

3) *Sia M un ideale massimale dell'anello A, tale che $\{1 + x \mid x \in M\} \subseteq U(A)$, allora A è un anello locale (e M è il suo unico ideale massimale).*

Dimostrazione. 1) M, come ogni ideale proprio, è contenuto in $A \setminus U(A)$; l'inclusione inversa segue dal punto (ii) della Proposizione 6 e dal fatto che M è l'unico ideale massimale di A.

2) Se $A \setminus M \subseteq U(A)$ allora ogni elemento non invertibile di A appartiene ad M, che pertanto contiene ogni ideale proprio di A, e dunque (per la Proposizione 6) è l'unico ideale massimale di A.

3) Sia M ideale massimale e supponiamo che per ogni $x \in M$, $1 + x$ sia invertibile in A. Sia $a \in A \setminus M$. Poiché M è massimale, $(M, a) = M + (a) = A$; in particolare esistono $x \in M$, $b \in A$ tali che $1 = x + ab$. Ma allora $ab = 1 - x \in U(A)$ e dunque a è anche'esso invertibile. Per il punto 2), si conclude che A è locale. □

Esercizio 2. [ex 1.12 in A.M.] un elemento e di un anello A si dice *idempotente* se $e^2 = e$. Si provi che i soli elementi idempotenti di un anello locale sono 0 e 1.

Esercizio 3. [ex 1.14 in A.M.] In un anello commutativo A sia Σ l'insieme degli ideali in cui tutti gli elementi non nulli sono divisori dello zero. Si provi che Σ ammette elementi massimali e che ogni elemento massimale di Σ è primo.

Esercizio 4. [$\sim$ ex 1.7 in A.M.] Si provi che ogni ideale primo di un anello finito è massimale. Più in generale, si provi che questo avviene in ogni anello A in cui per ogni $x \in A$ esistono interi $1 \leq n < m$ tali che $x^n = x^m$.

Esercizio 5. Sia $A \neq 0$ un anello; si provi che l'insieme degli ideali primi di A ha elementi minimali. [La soluzione si trova più avanti come dimostrazione del Lemma 18]

1.4 Radicale nilpotente e radicale di Jacobson

[anche questa parte è associata al capitolo 1 di A.M.]

Definizione. Un elemento a di un anello A si dice *nilpotente* se esiste $n \geq 0$ tale che $a^n = 0$.

Chiaramente, se A è un dominio d'integrità, 0 è il suo solo elemento nilpotente; ma non vale il viceversa: ad esempio, 0 è il solo elemento nilpotente di $\mathbb{Z}/6\mathbb{Z}$ (che non è un dominio d'integrità).

Se A è un anello, denotiamo con $\mathfrak{N}(A)$ l'insieme degli elementi nilpotenti di A, che chiameremo *radicale nilpotente*, o *nilradicale*, di A.

Proposizione 8. *$\mathfrak{N}(A)$ coincide con l'intersezione di tutti gli ideali primi di A. In particolare, $\mathfrak{N}(A)$ è un ideale di A e $A/\mathfrak{N}(A)$ non ha elementi nilpotenti diversi da 0.*

Dimostrazione. Denotiamo con P l'intersezione di tutti gli ideali primi di A.
Sia $x \in \mathfrak{N}(A)$ e sia J un ideale primo di A; allora $x + J$ è un elemento nilpotente del dominio d'integrità A/J e dunque $x + J = 0_{A/J} = J$ e quindi $x \in J$. Questo prova l'inclusione $\mathfrak{N}(A) \subseteq P$.
Viceversa, sia $x \in A \setminus \mathfrak{N}(A)$ e denotiamo con Σ l'insieme di tutti gli ideali I di A con la proprietà che non esiste $n \geq 1$ tale che $x^n \in I$; per la scelta di x, $(0) \in \Sigma$ (che dunque non è vuoto). Si verifica quindi immediatamente che, ordinato per inclusione, Σ è induttivo e dunque, per il Lemma di Zorn, ammette un elemento massimale M. Osservato che, poiché $A \notin \Sigma$, M è un ideale proprio, proviamo che è primo. Siano $a, b \in A$ con $ab \in M$ e supponiamo, per assurdo, $a \notin M$ e $b \notin M$; allora gli ideali $U_a = (a) + M$ e $U_b = (b) + M$ contengono propriamente M e quindi non appartengono a Σ. Esistono dunque interi $n, m \geq 1$ tali che $x^n \in U_a$ e $x^m \in U_b$; ma allora

$$x^{n+m} \in (ab) + M \subseteq M,$$

che è assurdo. Dunque M è primo e pertanto contiene P. Poiché $x \notin M$ si conclude che $x \notin P$, e la dimostrazione che $\mathfrak{N}(A)$ coincide con P.

Dunque $\mathfrak{N}(A)$ è un ideale. L'ultima affermazione è ora immediata; sia, per qualche $x \in A$ e $n \geq 1$, $(x + \mathfrak{N}(A))^n = 0$, allora $x^n \in \mathfrak{N}(A)$ e quindi, per qualche $m \geq 1$, $x^{nm} = (x^n)^m = 0$. Questo mostra che $x \in \mathfrak{N}(A)$ e quindi $x + \mathfrak{N}(A) = 0$. □

Esempio 2. Sia $2 \leq n \in \mathbb{N}$ e $A = \mathbb{Z}/nZ$. Gli ideali primi di A sono tutti e soli quelli del tipo $p\mathbb{Z}/n\mathbb{Z}$ al variare di p tra i divisori primi di n; dunque $\mathfrak{N}(A) = q\mathbb{Z}/n\mathbb{Z}$ dove q è il prodotto dei divisori primi distinti di n.

Esercizio 6. Si provi in modo diretto (cioè verificando soddisfa la definizione) che $\mathfrak{N}(A)$ è un ideale di A [per quanto riguarda la differenza di due elementi nilpotenti si adoperi la formula del binomio di Newton].

Un'utile osservazione [ex 1.1 in A.M.] riguardante gli elementi nilpotenti di un anello è la seguente:

Lemma 9. *Siano $u \in U(A)$ e $x \in \mathfrak{N}(A)$, allora $u + x \in U(A)$.*

Dimostrazione. Cominciamo con il mostrare che se $x \in \mathfrak{N}(A)$, allora $1 + x$ è invertibile. Infatti, esiste un intero *dispari* $n \geq 1$ tale che $x^n = 0$, e dunque

$$(1 + x)(x^{n-1} - x^{n-2} + \cdots - x + 1) = 1 + x^n = 1,$$

il che mostra che $1 + x$ è invertibile. Sia ora $u \in U(A)$ un generico elemento invertibile, allora ux è nilpotente e dunque, per quanto appena visto,

$$u + x = u(1 + u^{-1}x)$$

è un prodotto di elementi invertibili e pertanto è invertibile. □

Definizione. Sia $A \neq 0$ un anello commutativo, il *radicale di Jacobson* $\mathrm{J}(A)$ di A è l'intersezione di tutti gli ideali massimali di A.

Dalla Proposizione 8 segue immediatamente che, per ogni anello commutativo $A \neq 0$,

$$\mathfrak{N}(A) \subseteq \mathrm{J}(A).$$

Lemma 10. *Sia $x \in A \neq 0$; allora $x \in \mathrm{J}(A)$ se e solo se $1 - xy$ è invertibile per ogni $y \in A$.*

Dimostrazione. ($\Rightarrow$) Sia $x \in \mathrm{J}(A)$ e assumiamo, per assurdo, che esista $y \in A$ tale che $1 - xy$ non è invertibile. Allora $1 - xy \in M$ per qualche ideale massimale M; ma $x \in \mathrm{J}(A) \subseteq M$ e dunque si ha l'assurdo

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

($\Leftarrow$) Sia $x \notin \mathrm{J}(A)$. Allora $x \notin M$ per qualche ideale massimale M di A. Allora $A = (x) + M$ e, in particolare, esistono $y \in A$, $a \in M$ tali che $1 = xy + a$. Dunque $a = 1 - xy$ non è invertibile (poiché appartiene all'ideale proprio M). $\square$

1.5 Radicale di un ideale [pag 8, 9 in A.M.]

Sia I ideale dell'anello commutativo A, il *radicale* di I (denotato con $\sqrt{I}$ o con $rad(I)$) è definito come l'insieme di tuti gli elementi di A una cui potenza appartiene ad I:

$$\sqrt{I} = \{u \in A \mid \exists\ 1 \leq n \in \mathbb{N} \text{ con } x^n \in I\}.$$

Dunque, $I \subseteq \sqrt{I}$ e

$$\frac{\sqrt{I}}{I} = \mathfrak{N}\Big(\frac{A}{I}\Big),$$

cosa che, tra l'altro, fornisce una dimostrazione che $\sqrt{I}$ è un ideale di A e che $\sqrt{I}$ coincide con il proprio radicale; inoltre, dalla Proposizione 8 e dal Teorema di Corrispondenza segue la seguente definizione equivalente.

Proposizione 11. *Il radicale di un ideale proprio I di un anello A coincide con l'intersezione di tutti gli ideali primi di A che contengono I.*

Ad esempio, se $A = \mathbb{Z}$ e $n \geq 2$, $\sqrt{n\mathbb{Z}} = q\mathbb{Z}$ dove q è il prodotto dei divisori primi positivi distinti di n (vedi esempio 2).

Quanto osservato garantisce subito (i) e (ii) della seguente lista delle proprietà di base dei radicali [exercise 1.13 in A.M.]

Proposizione 12. *Siano I, J ideali dell'anello commutativo A. Allora,*

(i) $\sqrt{\sqrt{I}} = \sqrt{I}$;

(ii) $\sqrt{I} = A$ *se e solo se* $I = A$;

(iii) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;

(iv) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$;

(v) *Se I è primo e $n \geq 1$, allora* $\sqrt{I^n} = I$.

Per quel che riguarda (iii), l'inclusione $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$ è ovvia; viceversa, se $x \in \sqrt{I} \cap \sqrt{J}$, allora esistono $n, m \geq 1$ con $x^n \in I$, $x^m \in J$, e si ha pertanto $x^{n+m} = x^n x^m \in IJ$ e $x \in \sqrt{IJ}$.
Il punto (v) segue per induzione su n, infatti $\sqrt{I^n} = \sqrt{I^{n-1} \cap I} = \sqrt{I^{n-1}}$ e, se I è primo, $\sqrt{I} = I$.
Infine, per il punto (iv) possiamo assumere $I + J \neq A$ (il caso coprimo è infatti ovvio), ed osservare che se P è un ideale primo contenente $I + J$ allora I contiene $\sqrt{I}$ e $\sqrt{J}$,

e dunque (essendo un ideale) P contiene $\sqrt{I}+\sqrt{J}$. Quindi $\sqrt{I+J} \supseteq \sqrt{\sqrt{I}+\sqrt{J}}$, e poiché l'inclusione inversa è ovvia siamo a posto.

OSSERVAZIONE (in merito al punto (iv)): la somma di ideali primi non è necessariamente un ideale primo; ad esempio, (x) e $(x+4)$ sono ideali primi in $\mathbb{Z}[x]$ ma la somma $(x)+(x+4)=(x,4)$ non è primo. Quindi, in generale, vale l'inclusione $\sqrt{I}+\sqrt{J} \subseteq \sqrt{I+J}$, ma non l'uguaglianza.

Esercizio 7. Sia $\phi : A \to B$ un omomorfismo di anelli, e siano I un ideale di A e J un ideale di B. Si provino i seguenti fatti:

(1) $\phi(\sqrt{I}) \subseteq \sqrt{\phi(I)}$ (dando un esempio in cui l'inclusione risulta propria);

(2) $\phi^{-1}(\sqrt{J}) = \sqrt{\phi^{-1}(J)}$;

(3) se ϕ è suriettivo e A ha un numero finito di ideali massimali allora $\phi(\mathfrak{N}(A)) = \mathfrak{N}(B)$.

1.6 Esempi

Studiamo il radicale nilpotente e quello di Jacobson in alcuni casi significativi, indicando sempre con A un *anello commutativo*.

1. ANELLO DEI POLINOMI. [ex 1.2 e 1.4 in A.M.] $A[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in A.

Proposizione 13. *Sia* $f = a_0 + a_1x + \ldots + a_nx^n \in A[x]$

(i) *f è nilpotente in $A[x]$ se e solo se $a_0, a_1, \ldots, a_n$ sono elementi nilpotenti di A.*

(ii) *f è invertibile in $A[x]$ se e solo se $a_0 \in U(A)$ e $a_1, \ldots, a_n$ sono elementi nilpotenti di A.*

Dimostrazione. (i) Se $a_0, a_1, \ldots, a_n \in \mathfrak{N}(A)$ allora f è una somma di elementi nilpotenti in $A[x]$ e dunque è esso stesso nilpotente.
Per il viceversa, si assume $f \in \mathfrak{N}(A[x])$ si procede per induzione su n. Il caso $n=0$, cioè $f = a_0 \in A$ è ovvio. Sia $n \geq 1$, e sia $m \geq 1$ tale che $f^m = 0$; dallo sviluppo di quest'ultima identità si ricava $a_n^m x^{nm} = 0$, dunque $a_n^m = 0$ (quindi $a_n \in \mathfrak{N}(A)$) e inoltre $a_nx^n \in \mathfrak{N}(A[x])$. Ma allora

$$a_0 + \ldots + a_{n-1}x^{n-1} = f - a_nx^n$$

è un elemento nilpotente e, per ipotesi induttiva, $a_0, \ldots, a_{n-1} \in \mathfrak{N}(A)$.

(ii) Se $a_0 \in U(A) \subseteq U(A[x])$ e $a_1, \ldots, a_n \in \mathfrak{N}(A)$, allora per il punto precedente $a_1x + \ldots a_nx^n \in \mathfrak{N}(A[x])$ e per il Lemma 9 si ha che f è invertibile in $A[x]$.

Viceversa, sia $f \in U(A[x])$, $g = b_0 + b_1 x + \ldots + b_m x^m$ il suo inverso, e procediamo per induzione su $n = \deg f$. Dallo sviluppo dell'identità $fg = 1$ si ricava subito $a_0 b_0 = 1$; quindi $a_0 \in U(A)$, e in particolare abbiamo l'asserto per $n = 0$. Sia $n \geq 1$; per induzione su $r = 0, \ldots, m$ proviamo che

$$a_n^{r+1} b_{m-r} = 0. \tag{3}$$

Per $r = 0$, si ha $a_n^{0+1} b_{m-0} = a_n b_m = 0$ dallo sviluppo di $fg = 1$. Sia $r \geq 1$; osserviamo che $c = a_n b_{m-r} + a_{n-1} b_{m-(r-1)} + \cdots + a_{n+m-r} b_0$ è il coefficiente di x^{n+m-r} in fg e dunque $c = 0$; applicando quindi l'ipotesi induttiva,

$$a_n^{r+1} b_{m-r} = a_n^r c - a^r (a_{n-1} b_{m-(r-1)} + \cdots + a_{n+m-r} b_0) = 0 - 0 = 0.$$

Dunque vale la (3). In particolare $a_n^{m+1} b_0 = 0$; ma b_0 è invertibile, e quindi $a_n^{m+1} = 0$ e $a_n \in \mathfrak{N}(A)$. Allora $a_n x^n \in \mathfrak{N}(A[x])$ e, per il Lemma 9,

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} = f - a_n x^n$$

è invertibile. Applicando l'ipotesi induttiva si ha $a_1, \ldots, a_{n-1} \in \mathfrak{N}(A)$. □

Corollario 14. $\mathrm{J}(A[x]) = \mathfrak{N}(A[x])$.

Dimostrazione. L'inclusione $\mathfrak{N}(A[x]) \subseteq \mathrm{J}(A[x])$ è ovvia.
Viceversa, sia $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathrm{J}(A[x])$. Allora, per il Lemma 10,

$$1 + xf = 1 + a_0 x + a_1 x^2 + \ldots + a_n x^{n+1}$$

è invertibile e dunque, per il punto (ii) della Proposizione precedente, $a_0, \ldots, a_n$ sono elementi nilpotenti, e quindi, per il punto (i) della stessa, $f \in \mathfrak{N}(A[x])$. □

Esercizio 8. [ex 1.2(iii) in A.M.] Con le notazioni di cui sopra, si provi che $0 \neq f \in A[x]$ è un divisore dello zero in $A[x]$ se e solo se esiste $0 \neq a \in A$ tale che $af = 0$.

Esercizio 9. [Lemma di Gauss] Dato un ideale I dell'anello A, sia

$$I[x] = \{a_0 + a_1 x + \ldots a_n x^n \mid n \geq 0,\ a_0, a_1, \ldots a_n \in I\}.$$

Si provi che $I[x]$ è un ideale di $A[x]$, e che se I è un ideale primo di A allora $I[x]$ è un ideale primo di $A[x]$.

2. Anello delle serie formali. [∼ ex 1.5 in A.M.] Sia $A[[x]]$ l'anello delle *serie formali* a coefficienti in A (si veda la definizione nel capitolo 8 di [Alg 1] nel caso di coefficienti in un campo; l'estensione agli anelli commutativi è immediata).

Lemma 15. *Considerato un elemento $f \in A[[x]]$:*

$$f = \sum_{n\in\mathbb{N}} a_n x^n = a_0 + a_1 x + \ldots + a_n x^n + \cdots,$$

(i) *f è invertibile in $A[[x]]$ se e solo se a_0 è invertibile in A,*

(ii) *se f è nilpotente allora a_n è nilpotente per ogni $n \in \mathbb{N}$.*

Dimostrazione. (i) Se f è invertibile è immediato concludere che a_0 è un elemento invertibile di A. Viceversa, se $a_0 \in U(A)$, si pone $b_0 = a_0^{-1}$ e, induttivamente, per $n \geq 1$,

$$b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i};$$

si considera quindi $g = \sum_{n\in\mathbb{N}} b_n x^n$ e si verifica facendo i calcoli che $fg = 1$.

(ii) Supponiamo $f \in \mathfrak{N}(A[[x]])$ e sia $m \geq 1$ tale che $f^m = 0$. Allora $a_0^m = 0$ si ricava direttamente sviluppando f^m. Per provare che anche gli altri coefficienti a_n sono nilpotenti, si procede per induzione su n. Sia $n \geq 1$ e poniamo $g = \sum_{i\in\mathbb{N}} a_{n+i} x^i$; per ipotesi induttiva $a_0, \ldots, a_{n-1}$ sono nilpotenti e quindi $a_0 + a_1 x + \cdots a_{n-1} x^{n-1}$ è un elemento nilpotente di $A[[x]]$; di conseguenza

$$f - (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = \sum_{j\geq n} a_j x^j = x^n g$$

è nilpotente. Da ciò segue che g è nilpotente e quindi, come prima, che a_n, che è il termine di grado 0 di g, è nilpotente. □

In generale, l'implicazione (ii) nel Lemma 15 non si inverte (vedi, ad esempio, l'esercizio 19), tuttavia, anche così è sufficiente per trarre, in modo ovvio, la seguente conclusione.

Corollario 16. *Se $\mathfrak{N}(A) = (0)$ allora $\mathfrak{N}(A[[x]]) = (0)$.*

Proposizione 17. *Sia $\mathrm{J} = \mathrm{J}(A[[x]])$; allora*

(1) $\mathrm{J} = \left\{ \sum_{n\in\mathbb{N}} a_n x^n \mid a_o \in \mathrm{J}(A) \right\}$.

(2) $\mathrm{J} \neq \mathfrak{N}(A[[x]])$.

(3) *la funzione $\pi : A[[x]] \to A$ definita da $\pi(\sum a_n x^n) = a_0$ induce una corrispondenza biunivoca tra l'insieme degli ideali massimali di $A[[x]]$ e quelli di A; in particolare $A[[x]]$ è un anello locale se e solo se A è un anello locale.*

Dimostrazione. (1) Sia $f = \sum_{n\in\mathbb{N}} a_n x^n \in A[[x]]$. Se $f \in \mathrm{J}$ allora, per ogni $b \in A$, dal Lemma 10 segue che $1 - bf$ è invertibile in $A[[x]]$; quindi $1 - ba_0 \in U(A)$ per il Lemma 15. Applicando il Lemma 10 nell'altra direzione si conclude che a_0 appartiene a $\mathrm{J}(A)$.

Viceversa, sia $a_0 \in \mathrm{J}(A)$. Allora, per ogni $g = \sum_{n\in\mathbb{N}} b_n x^n \in A[[x]]$, il termine noto di $1 - fg$ è $1 - a_0 b_0$ che è invertibile in A. Per il punto (i) del Lemma 15, $1 - fg$ è invertibile in $A[[x]]$ e dunque, ancora una volta per il lemma 10, $f \in \mathrm{J}$.

(2) Basta osservare che, per il punto (1), $x \in \mathrm{J}$ mentre x non è nilpotente.

(3) Chiaramente, π è un omomorfismo suriettivo e $\ker \pi = (x)$. Ora, per il punto (1), ogni ideale massimale di $A[[x]]$ contiene (x); l'affermazione segue quindi immediatamente dal Teorema di corrispondenza. □

Esercizio 10. Si provi che se A è un dominio d'integrità allora $A[[x]]$ è un dominio d'integrità.

In particolare, se $\mathbb{K}$ è un campo, $\mathfrak{N}(\mathbb{K}[[x]] = (0)$ mentre, per la Proposizione 17, $\mathbb{K}[[x]]$ è un anello locale il cui unico ideale massimale è $\mathrm{J}(\mathbb{K}[[x]]) = \ker \pi = (x)$.
Semplici esempi di anelli locali in cui il nilradicale e il radicale di Jacobson coincidono, sono invece gli anelli $\mathbb{Z}/p^n\mathbb{Z}$, con p un primo e $n \geq 1$. Nel prossimo esempio, ne vedremo qualcuno più complicato.

3. Anelli gruppali. [questo non c'è in A.M.] Siano A un anello commutativo e G un gruppo (moltiplicativo). Si denota con $A[G]$ l'insieme delle espressioni formali

$$\alpha := \sum_{g\in G} \alpha(g) g$$

dove $\alpha(g) \in A$ per ogni $g \in G$ e solo un numero finito di $\alpha(g)$ sono diversi da zero.
Su tale insieme si definisce una addizione per componenti ed un prodotto (detto prodotto di *convoluzione*) che deriva dalla moltiplicazione nel gruppo G e dalla proprietà distributiva; precisamente, se $\beta = \sum_{g\in G} \beta(g) g \in A[G]$, allora

$$\alpha + \beta = \sum_{g\in G} (\alpha(g) + \beta(g)) g$$

$$\alpha \cdot \beta = \sum_{g\in G} \Big(\sum_{xy=g} \alpha(x)\beta(y) \Big) g.$$

Si verifica facilmente che, con tali operazioni, $A[G]$ è un anello, che si chiama *anello gruppale* (l'elemento identico è $1 = 1_A 1_G$); ed è cosa immediata convincersi che $A[G]$ è un anello commutativo se e soltanto se G è un gruppo abeliano. Si osservi anche che, per ogni $g, g' \in G$, $(1g)(1g') = 1(gg')$; dunque associando ad ogni $g \in G$ l'elemento $1g \in A[G]$ si definisce un omomorfismo iniettivo (di gruppi) da G nel gruppo degli elementi invertibili di $A[G]$.

Poiché ogni elemento $\alpha \in A[G]$ ha solo un numero finito di termini $\alpha(g) \neq 0$, risulta definita l'applicazione $\pi : A[G] \to A$ data da, per ogni $\alpha \in A[G]$,

$$\pi(\alpha) = \sum_{g \in G} \alpha(g).$$

Inoltre, π è un omomorfismo suriettivo di anelli (verifica per esercizio); il suo nucleo è un ideale, detto *ideale aumentante* di $A[G]$. Quindi

$$\ker \pi = \Big\{ \sum_{g \in G} \alpha(g) g \in A[G] \Big| \sum_{g \in G} \alpha(g) = 0 \Big\},$$

e, per il Teorema di omomorfismo, $A[G]/\ker \pi \simeq A$.

Ad esempio, se $\mathbb{K}$ è un campo e $G = \langle z \rangle$ un gruppo ciclico *infinito* (quindi G, scritto moltiplicativamente, è isomorfo al gruppo additivo $\mathbb{Z}$), allora l'anello gruppale $\mathbb{K}[G]$ non è altro che l'anello $\mathbb{K}[z, z^{-1}]$ dei polinomi di Laurent a coefficienti in $\mathbb{K}$.

Fissato un primo p, siano ora $\mathbb{K}$ un campo di caratteristica p e G un p-gruppo (cioè ogni elemento di G ha ordine una potenza di p) abeliano, e consideriamo l'anello gruppale $\mathbb{K}[G]$. Sia I il suo ideale aumentante, allora, poiché $\mathbb{K}[G]/I \simeq \mathbb{K}$ è un campo, I è un ideale massimale. Sia ora $\alpha = \sum_{g \in G} \alpha(g) g$ un generico elemento di I; tralasciando i termini uguali a zero, possiamo scrivere $\alpha = \alpha_1 g_1 + \cdots + \alpha_n g_n$, per un insieme finito $g_1, \dots g_n$ di elementi di G, e inoltre $\alpha_1 + \cdots + \alpha_n = 0$. Per l'ipotesi sul gruppo G, esiste $t \geq 1$ tale che $g_i^{p^t} = 1_G$ per ogni $i = 1, \dots, n$. Ora, poiché $\mathbb{K}$ ha caratteristica p, $\mathbb{K}[G]$ è un anello commutativo di caratteristica p, quindi l'elevazione alla potenza p^t è un omomorfismo di $\mathbb{K}[G]$. In particolare, si ha

$$\alpha^{p^t} = \alpha_1^{p^t} g_1^{p^t} + \cdots + \alpha_n^{p^t} g_n^{p^t} = (\alpha_1^{p^t} + \cdots + \alpha_n^{p^t}) 1_G = (\alpha_1 + \cdots + \alpha_n)^{p^t} 1_G = 0,$$

provando che α è nilpotente. Quindi $I \subseteq \mathfrak{N}(\mathbb{K}[G])$. Poiché, come osservato sopra, I è un ideale massimale, si ha anche $\mathrm{J}(\mathbb{K}[G]) \subseteq I$. Dunque

$$I = \mathrm{J}(\mathbb{K}[G]) = \mathfrak{N}(\mathbb{K}[G]);$$

in particolare, $\mathbb{K}[G]$ è un anello locale e I il suo unico ideale massimale.

Esercizio 11. Siano A un anello e G un gruppo (commutativo). Si provi che l'ideale aumentante dell'anello gruppale $A[G]$ è l'ideale generato dall'insieme $\{1 - g \mid g \in G\}$.

Esercizio 12. [$\sim$ ex 1.6 in A.M.] Sia A un anello tale che ogni ideale non contenuto in $\mathfrak{N}(A)$ contiene un idempotente $\neq 0$. Si provi che $\mathfrak{N}(A) = \mathrm{J}(A)$.

Esercizio 13. [$\sim$ ex 1.10 in A.M.] Sia $A \neq 0$ anello commutativo e si assuma che A contenga un unico ideale primo P. Si provi che $P = \mathfrak{N}(A)$ è un ideale massimale.

Appendice: Spettro di un anello [ex 1.15 – 1.18 in A.M.]

In questa sezione, A è un anello, $A \neq (0)$.

Si denota con $Spec(A)$ l'insieme degli ideali primi di A: dotato della topologia di Zariski, che definiremo tra poco, si chiama *spettro di A* ("prime spectrum" in A.M.)
Prima osserviamo che $Spec(A)$ non è vuoto e che, quando visto come insieme ordinato per inclusione, contiene elementi massimali (che sono gli ideali massimali di A); inoltre si ha la seguente

Lemma 18. [ex 1.8 in A.M.] *$Spec(A)$ contiene elementi minimali.*

Dimostrazione. Sia $(J_\lambda)_{\lambda\in\Lambda}$ una catena di ideali primi di A, allora $J = \bigcap_{\lambda\in\Lambda} J_\lambda$ è un ideale di A; proviamo che è primo. Siano $x, y \in A$ con $xy \in J$ e $x \notin J$; allora esiste $i \in \Lambda$ tale che $x \notin J_i$. Ma allora $x \notin J_\lambda$ per ogni λ tale che $J_\lambda \subseteq J_i$. Poiché gli ideali J_λ sono primi e formano una catena si ha:

$$y \in \bigcap\{J_\lambda \mid J_\lambda \subseteq J_i\} = J.$$

Quindi $J \in Spec(A)$. Applicando il Lemma di Zorn a $Spec(A)$ ordinato per inclusione inversa, si conclude che $Spec(A)$ ammette elementi minimali. □

Topologia di Zariski. Per ogni ideale I di A si definisce

$$V(I) = \{P \in Spec(A) \mid I \subseteq P\}.$$

Quindi, poiché ogni ideale proprio è contenuto in un ideale primo, $V(I) = \emptyset$ se e solo se $I = A$; inoltre, per la Proposizione 8, $V(I) = Spec(A)$ se e solo se $I \subseteq \mathfrak{N}(A)$, e, per la Proposizione 11, $V(I) = V(\sqrt{I})$ per ogni ideale I.

Le seguenti proprietà sono anch'esse di verifica immediata (per la (1) si veda il punto (iii) della Proposizione 12).

Lemma 19. (1) *Se I, J sono ideali di A,*

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

(2) *Se $(I_\lambda)_{\lambda\in\Lambda}$ una famiglia di ideali di A, e I l'ideale generato da $\bigcup_{\lambda\in\Lambda} I_\lambda$,*

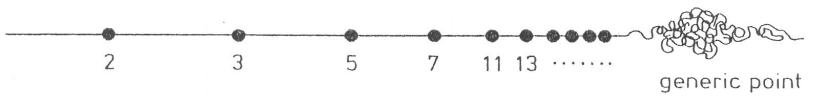
$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V(I).$$

Sia $\mathsf{C} = \{V(I) \mid I \text{ ideale di } A\}$; per il Lemma appena enunciato e le osservazioni precedenti che, in particolare, assicurano $\emptyset, Spec(A) \in \mathsf{C}$, C soddisfa le condizioni che ne fanno l'insieme dei *chiusi* di una topologia su $Spec(A)$, detta, appunto, *Topologia di Zariski.*

In particolare, osserviamo che per ogni $I \in Spec(A)$ la chiusura di $\{I\}$ nella topologia di Zariski è $V(I)$, e che I è un ideale massimale se e solo se $\{I\}$ è chiuso; più in generale, che dati due punti I e J in $Spec(A)$, I appartiene alla chiusura di $\{J\}$ se e solo se $J \subseteq I$. Da ciò segue facilmente che $Spec(A)$ è uno spazio che soddisfa la condizione di separazione T_0 (ovvero dati due punti distinti esiste un aperto che ne contiene uno ed uno solo): infatti se I e J sono ideali primi distinti di A si ha, eventualmente scambiandoli, $I \not\subseteq J$ e dunque J appartiene al complementare in $Spec(A)$ di $V(I)$, che è un aperto. [ex 1.18 in A.M.]

Esempi. [ex 1.16 in A.M.] • Se $\mathbb{K}$ è un campo, $Spec(\mathbb{K})$ consiste in un unico punto.

• $Spec(\mathbb{Z})$ consiste in un'infinità numerabile di punti chiusi, corrispondenti agli ideali $p\mathbb{Z}$ con p primo, e di un punto 'generico', corrispondente all'ideale (0), la cui chiusura è tutto lo spazio.



visualizzazione di $Spec(\mathbb{Z})$ da una lezione di David Mumford.

• Se $\mathbb{K}$ è un campo, gli ideali primi di $\mathbb{K}[x]$ sono l'ideale nullo (0) e gli ideali massimali (e questi ultimi sono in corrispondenza biunivoca con i polinomi irriducibili monici), inoltre, ogni ideale proprio è contenuto in un numero finito di ideali massimali. Quindi i chiusi di $Spec(\mathbb{K}[x])$ sono i sottoinsiemi finiti di punti (ideali massimali) associati a polinomi irriducibili e l'intero spazio (che è la chiusura del punto (0)).
Se $\mathbb{K}$ è algebricamente chiuso, gli ideali massimali, e quindi i punti chiusi in $Spec(\mathbb{K}[x])$, sono tutti e soli quelli del tipo $(x - a)$ al variare di a in $\mathbb{K}$; a questi, a completare l'insieme $Spec(\mathbb{K}[x])$, si aggiunge il punto generico (0).
Se $\mathbb{K} = \mathbb{R}$oltre a quelli di grado 1, ci sono polinomi irriducibili di grado 2, i quali generano comunque un ideale massimale, quindi un punto chiuso in $Spec(\mathbb{R}[x])$.

• $Spec(\mathbb{Z}[x])$ è più complesso, e - forse - ci torneremo più avanti.

Scriviamo, in quanto segue, $\mathsf{X} = Spec(A)$. Per ciascun $f \in A$ poniamo

$$\mathsf{X}_f = \{P \in \mathsf{X} \mid f \notin P\}.$$

Poiché, chiaramente, $\mathsf{X}_f = \mathsf{X} \setminus V((f))$, X_f è un aperto nella topologia di Zariski per ogni $f \in A$. Di fatto ogni aperto di tale topologia è della forma $\mathsf{X} \setminus V(I)$, quindi è l'unione della famiglia di aperti $(\mathsf{X}_f)_{f \in I}$. Quindi, l'insieme $\{\mathsf{X}_f \mid f \in A\}$ è una *base* (di aperti) per la topologia di Zariski. Valgono inoltre le seguenti proprietà:

Lemma 20. [ex 1.17 in A.M.] *Posto* $\mathsf{X} = Spec(A)$*, siano* $f, g \in A$*. Allora*

(i) $\mathsf{X}_f = \mathsf{X}$ *se e solo se* $f \in U(A)$*;*

(ii) $\mathsf{X}_f = \emptyset$ *se e solo se* $f \in \mathfrak{N}(A)$*;*

(iii) $\mathsf{X}_{fg} = \mathsf{X}_f \cap \mathsf{X}_g$*;*

(iv) $\mathsf{X}_f = \mathsf{X}_g$ *se e solo se* $\sqrt{(f)} = \sqrt{(g)}$*.*

Dimostrazione. Tutto discende agevolmente dal fatto, ovvio, che per ogni $f \in A$ ed ogni $P \in \mathsf{X}$,

$$P \in \mathsf{X}_f \;\Leftrightarrow\; P \notin V((f)) = V(\sqrt{(f)})$$

e dalle proprietà dei chiusi $V(I)$ (il Lemma 19 e i commenti che lo precedono). □

Proposizione 21. [ex 1.17 in A.M.] *Sia* $A \neq 0$ *e* $\mathsf{X} = Spec(A)$*.*

(1) *Sia* $\emptyset \neq S \subseteq A$*; allora* $\bigcup_{f\in S} \mathsf{X}_f = \mathsf{X}$ *se e solo ste* A *coincide con l'ideale* (S) *generato da* S*.*

(2) X *è uno spazio compatto.*

Dimostrazione. (1) X coincide con l'unione $\bigcup_{f\in S} \mathsf{X}_f = \mathsf{X}$ se e soltanto se per ogni ideale primo P di A esiste $f \in S$ tale che $f \notin P$. Questo equivale a dire che (S) non è contenuto in alcun ideale primo, e quindi che coincide con A.

(2) Vogliamo provare che da ogni ricoprimento aperto di X è possibile estrarre un sottoricoprimento finito. È chiaro che possiamo assumere che il ricoprimento iniziale sia realizzato da aperti appartenenti alla base $\{\mathsf{X}_f \mid f \in A\}$, e quindi che

$$\mathsf{X} = \bigcup_{f\in S} \mathsf{X}_f$$

per qualche sottoinsieme non vuoto S di A. Per il punto (1), si ha che 1 appartiene all'ideale generato da S; dunque esiste un sottoinsieme finito $\{f_1, \ldots, f_n\} \subseteq S$ tale che $a_1 f_1 + \ldots + a_n f_n = 1$, con $a_i \in A$. Ma allora $1 \in (f_1, \ldots, f_n)$, quindi $A = (f_1, \ldots, f_n)$ e

$$\mathsf{X} = \bigcup_{i=1}^{n} \mathsf{X}_{f_n}.$$

Pertanto X è uno spazio compatto. □

Esercizio 14. Si provi che, per ogni $f \in A$, X_f è un compatto.

Esercizio 15. [ex 1.19 in A.M.] Uno spazio topologico T è *irriducibile* se $T \neq \emptyset$ e ogni coppia di aperti non vuoti di T ha intersezione non vuota. Sia $A \neq 0$; si provi che $Spec(A)$ è uno spazio irriducibile se e solo se $\mathfrak{N}(A)$ è un ideale primo.

Soluzioni di alcuni esercizi.

Esercizio 2 – Soluzione. Sia A un anello locale, M il suo (unico) ideale massimale e $\mathbb{K} = A/M$ il campo residuo. Sia e un elemento idempotente di A. Se $e \notin M$ allora e è invertibile e $1 = ee^{-1} = e^2e^{-1} = e$. Se invece $e \in M$ si ha $1 - e \notin M$ e

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e;$$

dunque $1 - e$ è idempotente, quindi, per il caso precedente, $1 - e = 1$, e $e = 0$. ∎

Esercizio 3 – Soluzione. Σ è un insieme ordinato per inclusione e non è vuoto, poiché $(0) \in \Sigma$. Sia $(J_\lambda)_{\lambda\in\Lambda}$ una catena in $(\Sigma, \subseteq)$; allora chiaramente $\bigcup_{\lambda\in\Lambda} J_\lambda$ appartiene a Σ. Possiamo quindi applicare il Lemma di Zorn per affermare che $(\Sigma, \subseteq)$ contiene un elemento massimale M, e $M \neq A$ (dato che $1 \notin M$). Proviamo che M è primo. Siano $x, y \in A$ con $xy \in M$ e supponiamo, per assurdo, che $x \notin M$ e $y \notin M$; allora né $(x) + M$ né $(y) + M$ appartengono a Σ, dunque esistono $a \in (x) + M$, $b \in (y) + M$ che non sono divisori dello zero di A. Ma $ab \in (xy) + M = M$ e dunque $ab = 0$ oppure ab è un divisore dello zero, fatto che porta alla conclusione assurda che uno tra a e b è divisore dello zero. ∎

Esercizio 4 – Soluzione. Basta chiaramente provare la seconda (e più generale) affermazione. Sia dunque A un anello tale che per ogni $x \in A$ esistono $1 \leq n < m$ con $x^n = x^m$, e sia P un ideale primo di A. Per $x \in A$ denotiamo con $\bar{x} = x + P \in A/P$. Sia $x \in A \setminus P$, allora per ipotesi esistono $1 \leq n < m$ con

$$0 = \bar{x}^m - \bar{x}^n = \bar{x}^n(\bar{x}^{m-n} - 1).$$

Poiché A/P è un dominio d'integrità e $\bar{x} \neq 0$, si ha $\bar{x}^{m-n} - 1 = 0$, ovvero $\bar{x}^{m-n} = 1$, e questo implica, dato che $m - n \geq 1$, che $\bar{x} = x + P$ è invertibile. Dunque A/P è un campo e pertanto P è un ideale massimale. ∎

Esercizio 8 – Soluzione. Sia $f = a_0 + a_1x + \ldots + a_nx^n$ con $a \neq 0$ un divisore dello zero in $A[x]$ e sia $g = b_0 + b_1x + \ldots + b_mx^m \in A[x]$, con $b_m \neq 0$, di grado minimo tale che $fg = 0$. Allora, $a_nb_m = 0$; quindi $\deg(a_ng) < \deg(g)$ e, poiché $(a_ng)f = 0$, $a_ng = 0$ per la scelta di g. Per $0 \leq r \leq n - 1$, supponiamo di aver provato che $a_{n-i}g = 0$ per ogni $0 \leq i \leq r$; allora, il coefficiente di grado $n + m - (r + 1)$ di $fg = 0$ è

$$0 = \sum_{i+j=n+m-(r+1)} a_ib_j = \sum_{j>r}^{n} a_{n-j}b_{m-(r+1)+j} = a_{n-(r+1)}b_m,$$

e quindi, come prima, $a_{n-(r+1)}g = 0$. Concludiamo quindi il ragionamento per induzione ricavando $a_ig = 0$ per ogni $i = 0, \ldots n$. Ma allora, in particolare, $a_ib_m = 0$ per ogni $i = 0, \ldots n$, e dunque $b_mf = 0$. Quindi $g = b_m \in A$. ∎

Esercizio 11 – Soluzione. Denotiamo con I l'ideale aumentante di $A[G]$ e con M l'ideale generato da $\{1_G - g \mid g \in G\}$. Chiaramente, $M \subseteq I$. Viceversa, sia $u \in I$; allora esistono $a_1, \ldots, a_n \in A$, $g_1, \ldots, g_n \in G$ con $u = a_1 g_1 + \ldots + a_n g_n$ e $a_1 + \ldots + a_n = 0$. Quindi

$$u = a_1 g_1 + \ldots + a_n g_n - (a_1 + \ldots + a_n)1_G = a_1(g_1 - 1_G) + \ldots + a_n(g_n - 1_G) \in I,$$

come si voleva. ∎

Esercizio 12 – Soluzione. Sia A come nelle ipotesi e supponiamo per assurdo $\mathfrak{N}(A) \neq \mathrm{J}(A)$. Allora esiste $a \in \mathrm{J}(A) \setminus \mathfrak{N}(A)$, dunque per ipotesi l'ideale (a) contiene un idempotente $e \neq 0$. Ora, $e^2 = e \neq 0$ implica in particolare che e non è nilpotente, quindi $e \notin \mathfrak{N}(A)$; ciò significa che esiste un ideale primo P di A con $e \notin P$. Siccome $e + P \neq 0_{A/P}$ è idempotente nel dominio d'integrità A/P, si deve avere $e + P = 1_{A/P} = 1 + P$. Segue che, se M è un ideale massimale contenente P, $e \notin M$, contro l'ipotesi $a \in \mathrm{J}(A)$. ∎

Esercizio 15 – Soluzione. Sia $\mathsf{X} = \mathit{Spec}(A)$, e $N = \mathfrak{N}(A)$, ed osserviamo che, per ogni $f \in A$, $\mathsf{X}_f \neq \emptyset$ se e solo se $f \notin N$.
Sia X irriducibile, e siano $a, b \in A$ tali che $a, b \in A \setminus N$; allora, per il punto (iii) del Lemma 20,

$$\mathsf{X}_{ab} = \mathsf{X}_a \cap \mathsf{X}_b \neq \emptyset,$$

e dunque $ab \notin N$, provando che N è primo.
Viceversa, sia N primo, e siano $a, b \in A$ tale che X_a e X_b non sono vuoti; allora $a, b \notin N$, dunque $ab \notin N$, e quindi $\mathsf{X}_a \cap \mathsf{X}_b \neq \emptyset$. Poiché la famiglia degli insiemi X_f $(f \in A)$ è una base di aperti, questo dimostra che X è irriducibile. ∎

2 Moduli

[questa parte è associata al capitolo 2 di A.M.]

2.1 Definizioni

Sia A un anello commutativo. Un A-**modulo** è un gruppo abeliano M (la cui notazione sarà sempre quella additiva) assieme ad un prodotto scalare

$$\begin{aligned} A \times M &\to M \\ (a, x) &\mapsto ax \end{aligned}$$

che verifica le seguenti proprietà. Per ogni $a, b \in A$ ed ogni $x, y \in M$,

- $a(x + y) = ax + ay$;
- $(a + b)x = ax + bx$;
- $(ab)x = a(bx)$;
- $1_A x = x$.

Esempi. 1) Ogni ideale dell'anello A è, nel modo naturale, un A-modulo; in particolare A è un A-modulo. Similmente, ogni quoziente A/I è un A-modulo.

2) Se $\mathbb{K}$ è un campo, i $\mathbb{K}$-moduli sono gli spazi vettoriali su $\mathbb{K}$ ($\mathbb{K}$-spazi).

3) Ogni gruppo abeliano è uno $\mathbb{Z}$-modulo.

4) Questo lo abbiamo visto nella prima parte, nel corso della dimostrazione del Teorema della Base normale. Sia $A = \mathbb{K}[x]$ con $\mathbb{K}$ un campo, e siano V un $\mathbb{K}$-spazio vettoriale e $\phi \in End_{\mathbb{K}}(V)$ una fissata applicazione lineare $V \to V$. Allora, porre, per ogni $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[x]$ ed ogni $v \in V$,

$$f(x) \cdot v = f(\phi)(v) = a_0 v + a_1 \phi(v) + \cdots + a_n \phi^n(v),$$

definisce un prodotto scalare che rende V un A-modulo. Si provi che ogni A-modulo si ottiene in questo modo.

Nota. Se M è un gruppo abeliano (additivo), allora l'insieme $End(M)$ (gli omomorfismi di gruppo da M in se stesso) è un anello rispetto alle operazioni di somma puntuale e composizione di applicazioni (questo anello non è in genere commutativo). Assegnare al gruppo M una struttura di A- modulo significa in sostanza considerare un omomorfismo di anelli $A \to End(M)$.

Definizione. Siano A un anello e M un A-modulo. Un sottoinsieme $M' \subseteq M$ è un A-*sottomodulo* di M se è un sottogruppo del gruppo additivo ed inoltre $a \cdot x \in M'$ per ogni $a \in A$ e ogni $x \in M'$.

Ad esempio, gli A-sottomoduli dell'anello A come modulo su se stesso sono gli ideali di A (come anello); gli $\mathbb{Z}$-sottomoduli di un gruppo abeliano G, sono i sottogruppi di G. Le seguenti proprietà sono di immediata verifica.

Proposizione 22. *Siano A un anello e M un A-modulo.*

(1) *Se M_1, M_2 sono A-sottomoduli allora $M_1 + M_2 = \{x + y \mid x \in M_1, y \in M_2\}$ è un A-sottomodulo di M.*

(2) *Se $\mathcal{N}$ è una famiglia di A-sottomoduli di M, allora $\bigcap_{N \in \mathcal{N}} N$ è un A-sottomodulo di M.*

Dal punto (2) discende, come sempre, che per ogni sottoinsieme X di un A-modulo M esiste un minimo A-sottomodulo di M che contiene X (il sottomodulo *generato* da X). Su questo torneremo nella prossima sezione; per il momento, proseguiamo con le definizioni di base, passando ai quozienti e agli omomorfismi.

Definizione. Siano A un anello, M un A-modulo e N un A-sottomodulo di M. Allora l'insieme quoziente (come gruppo abeliano),

$$\frac{M}{N} = \{x + N \mid x \in M\}$$

eredita naturalmente una natura di A-modulo mediante il prodotto scalare

$$a \cdot (x + N) = a \cdot x + N$$

per ogni $a \in A$ e $x + N \in M/N$. Tale A-modulo è il *modulo quoziente* di M su N.

Definizione. Siano A un anello e M, N due A-moduli. Un'applicazione $\phi : M \to N$ è un *omomorfismo di A-moduli* (o, anche, è *A-lineare*) se è un omomorfismo di gruppi additivi (cioè $\phi(x + y) = \phi(x) + \phi(y)$ per ogni $x, y \in M$) e

$$\phi(ax) = a\phi(x)$$

per ogni $a \in A$ e $x \in M$.

Fissato l'anello A, si verifica banalmente che la composizione di omomorfismi di A-moduli è un omomorfismo di A-moduli. Inoltre, se un omomorfismo $\phi : M \to N$ di A-moduli è una biezione, allora l'applicazione inversa $\phi^{-1} : N \to M$ è un omomorfismo di A-moduli; in tal caso si dice che ϕ è un *isomorfismo* di A-moduli; due A-moduli M e N sono *isomorfi* (o A-isomorfi) se esiste un isomorfismo $M \to N$ di A-moduli: in tal caso scriveremo $M \simeq_A N$.

Come per omomorfismi di gruppi e di anelli (e sostanzialmente con la stessa dimostrazione) sussiste poi il *Teorema di omomorfismo* (per A-moduli).

Teorema 23. *Sia A un anello e sia $\phi : M \to N$ un omomorfismo di A-moduli. Allora*

(1) $\ker(\phi) = \{x \in M \mid \phi(x) = 0_N\}$ *e* $\mathrm{Im}(\phi) = \{\phi(x) \mid x \in M\}$ *sono A-sottomoduli, rispettivamente, di M e di N.*

(2) *Si ha:* $M/\ker(\phi) \simeq_A \mathrm{Im}(\phi)$.

Da cui seguono il secondo e terzo Teorema di omomorfismo, che includiamo in un'unica Proposizione, la cui dimostrazione è lasciata per esercizio (si seguano quelle delle analoghe proprietà per gruppi).

Proposizione 24. *Siano A un anello, M un A-modulo e N, L due sottomoduli. Allora*

(1) *$N \cap L$ è un A-sottomodulo di L e $(N + L)/N \simeq_A L/(N \cap L)$.*

(2) *Se $L \subseteq N$, si ha*
$$\frac{M}{N} \simeq_A \frac{M/L}{N/L}.$$

Siano A un anello e M, N due A-moduli; poiché l'applicazione nulla da M in N (quella definita da $x \mapsto 0_N$ per ogni $x \in M$) è banalmente A-lineare, l'insieme

$$Hom_A(M, N) = \{\phi \mid \phi : M \to N \text{ applicazione } A\text{-lineare}\}$$

non è vuoto. Inoltre, esso è un A-modulo, mediante le operazioni definite naturalmente "per punti"; ovvero ponendo, per ogni $\phi, \psi \in Hom_A(M, N)$, $a \in R$ ed ogni $x \in M$:

$$(\phi + \psi)(x) = \phi(x) + \psi(x), \qquad (a \cdot \phi)(x) = a \cdot \phi(x).$$

Se poi $\phi : M \to M'$, $\psi : N \to N'$, sono omomorfismi di A-moduli, la composizione

$$\alpha \mapsto \psi \circ \alpha \circ \phi$$

definisce un omomorfismo di A-moduli $Hom_A(M', N) \to Hom_A(M, N')$ (e similmente si trova un omomorfismo di A-moduli $Hom_A(N', M) \to Hom_A(N, M')$).

Definizione. Siano M un A-modulo e N, L sottomoduli; si pone, in A,

$$(N : L) = \{a \in A \mid aL \subseteq n\}.$$

Si verifica molto facilmente che $(N : L)$ è un ideale di A. In particolare, per ogni sottomodulo N di M,

$$Ann_A(N) = (0 : N) = \{a \in A \mid ax = 0 \ \forall x \in N\}$$

è un ideale di A detto *annullatore* di N. Il modulo M si dice *fedele* se $Ann_A(M) = 0$. Un'osservazione utile è che se N è un A-sottomodulo di M e $I = Ann_A(M)$, allora N è in modo naturale, ponendo $(a + I) \cdot x = a \cdot x$ (per ogni $a + I \in A/I$ ed ogni $x \in N$) un (A/I)-modulo fedele.
Nel seguito questa notazione la utilizzeremo prevalentemente per un anello A come modulo su se stesso; in tal caso si applica a ideali I, J di A (quindi $(I : J) = \{a \in A \mid aJ \subseteq I\}$). Osserviamo che se X è un insieme di generatori di un A-modulo M, allora $Ann_A(M) = \{a \in A \mid ax = 0 \ \forall x \in X\}$; questo vale anche per ideali dell'anello A, per cui - ad esempio - se I è ideale di A e $x \in A$, scriveremo $(I : x) = (I : Ax)$.

Esercizio 16. Siano A un anello e M un A-modulo. Si provi che $Hom_A(A, M) \simeq_A M$.

Esercizio 17. [Exercise 1.12 in A.M.] Siano I, J, L ideali di un anello A; si provi che

(1) I $\subseteq (I : J)$ e $(I : J)J \subseteq I$;
(2) $((I : J) : L) = (I : JL) = (I : L) : J)$;
(3) $((I \cap J) : L) = (I : L) \cap (J : L)$;
(4) $(I : (J + L)) = (I : J) \cap (I : L)$.

2.2 Somme, prodotti, sequenze esatte

Sia A un anello e siano $M_1, M_2, \ldots M_n$ un numero finito di A-moduli. La *somma diretta*

$$M_1 \oplus M_2 \oplus \ldots \oplus M_n$$

è lo A-modulo definito a partire dal gruppo abeliano (additivo) $M_1 \times M_2 \times \ldots \times M_n$ mediante il prodotto scalare:

$$a \cdot (x_1, x_2, \ldots, x_n) = (a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n)$$

per ogni $a \in A$ e ogni $(x_1, x_2, \ldots, x_n) \in M_1 \times M_2 \times \ldots \times M_n$.
Se M è un A-modulo e $n \geq 1$, si denota con M^n la somma diretta di n copie di M,

$$M^n = M \oplus M \oplus \ldots \oplus M \quad (n \text{ termini}).$$

Vi sono due modi importanti - e collegati - per estendere la nozione di somma diretta a famiglie infinite di moduli. Siano quindi A un anello e $\{M_i\}_{i \in I}$ una famiglia di A-moduli

Definizione 1. Il *Prodotto diretto* della famiglia $\{M_i\}_{i \in I}$ è lo A-modulo, denotato con

$$\prod_{i \in I} M_i,$$

i cui elementi sono tutte le funzioni $m : I \to \bigcup_{i\in I} M_i$ tali che $m_i = m(i) \in M_i$ per ogni $i \in I$ (e può aiutare denotare tali funzioni come $m = (m_i)_{i\in I}$), provvisto delle operazioni - interna ed esterna - definite per componenti, ovvero

$$(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}, \qquad a \cdot (m_i)_{i\in I} = (a \cdot m_i)_{i\in I},$$

per ogni $(m_i)_{i\in I}, (m'_i)_{i\in I} \in \prod_{i\in I} M_i$ ed ogni $a \in A$.

Definizione 2. La *Somma diretta* dei moduli della famiglia $\{M_i\}_{i\in I}$ è lo A-sottomodulo del prodotto diretto, costituito dagli elementi di questo che sono quasi ovunque nulli,

$$\bigoplus_{i\in I} M_i = \Big\{(m_i)_{i\in I} \in \prod_{i\in I} M_i \big| m_i \neq 0 \text{ per un insieme finito di indici } i\Big\}.$$

Esempio. Per ogni $i \in \mathbb{N}$ sia $A_i = A$ come A-modulo. L'applicazione $\bigoplus_{i\in\mathbb{N}} A_i \to A[x]$ definita da

$$(a_0, a_1, a_2, \ldots) \mapsto a_0 + a_1 x + a_2 x^2 + \ldots$$

stabilisce un isomorfismo di A-moduli. Similmente si ha $\prod_{i\in\mathbb{N}} A \simeq_A A[[x]]$ (come A-moduli; perché $\prod_{i\in\mathbb{N}} A$ è anche in modo naturale un anello, che non è isomorfo all'anello delle serie formali).

Esercizio 18. Sia M un A-modulo, e siano N, L sottomoduli tali che $N + L = M$ e $N \cap L = 0$. SI provi che $M \simeq_A N \oplus L$.

Esercizio 19. Sia p un numero primo e, per ogni $n \geq 0$, $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Sia A il prodotto diretto degli anelli A_n. Si provi che in $A[[x]]$ esistono elementi non nilpotenti i cui coefficienti sono tutti elementi nilpotenti di A.

Definizione. Sia A un anello; una sequenza di A-moduli e applicazioni A-lineari

$$\ldots \longrightarrow M_{i-1} \xrightarrow{\nu_i} M_i \xrightarrow{\nu_{i+1}} M_{i+1} \longrightarrow$$

si dice *esatta* in M_i se $\ker(\nu_{I+1}) = \mathrm{Im}(\nu_i)$, e si dice *esatta* se è esatta in ogni M_i.

Da questa definizione segue, in particolare, che se $\phi : M \to N$ è un omomorfismo di A-moduli, allora

- dire che ϕ è iniettivo equivale a dire che la sequenza $0 \longrightarrow M \xrightarrow{\phi} N$ è esatta;
- dire che ϕ è suriettivo equivale a dire che la sequenza $M \xrightarrow{\phi} N \longrightarrow 0$ è esatta.

Une sequenza esatta del tipo

$$0 \longrightarrow N \xrightarrow{\nu} M \xrightarrow{\phi} L \longrightarrow 0$$

si dice *sequenza esatta corta* di A-moduli. Per quanto appena osservato, questo equivale a chiedere che ν sia un omomorfismo iniettivo - quindi $im(\nu) \simeq_A M$ - e che ϕ sia un omomorfismo suriettivo (che induce un A-isomorfismo $M/\mathrm{Im}(\nu) \simeq_A N$).

ESEMPIO. Fissato un numero primo p, per ogni $n \geq 1$ sia $P_n = \mathbb{Z}/p^n\mathbb{Z}$ come $\mathbb{Z}$-modulo e sia $\nu_n : P_{n+1} \to P_n$ definito da $\nu_n(x + p^{n+1}\mathbb{Z}) = p^{[n/2]}x + p^n\mathbb{Z}$, per ogni $z \in \mathbb{Z}$ (dove $[n/2]$ è la parte intera di $n/2$). Allora (facile esercizio)

$$\ldots \xrightarrow{\nu_4} P_4 \xrightarrow{\nu_3} P_3 \xrightarrow{\nu_2} P_2 \xrightarrow{\nu_1} P_1 \longrightarrow 0$$

è una sequenza esatta di Z-moduli.

ESEMPIO. Siano $M_1, \ldots, M_n$ A-moduli. Ponendo, per ogni n-upla $x_1, \ldots, x_n$, con $x_i \in M_i$, $\nu(x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, 0)$ e $\phi(x_1, \ldots, x_n) = x_n$, si ha che

$$0 \longrightarrow \bigoplus_{i=1}^{n-1} M_i \xrightarrow{\nu} \bigoplus_{i=1}^{n} M_i \xrightarrow{\phi} M_n \longrightarrow 0$$

è una sequenza esatta corta di A-moduli.

Esercizio 20. [Proposition 2.9 in A.M.] Sia $\phi : M \to M'$ un omomorfismo di A-moduli; per ogni A-modulo N, rimane associato, mediante composizione, l'omomorfismo di A-moduli $\bar{\phi} : Hom_A(M', N) \to Hom_A(M, N)$ (dunque, $\bar{\phi}(\nu) = \nu \circ \phi$ per ogni $\nu \in Hom_A(M', N)$). Sia provi che una sequenza di omomorfismi di A-moduli

$$M' \xrightarrow{\phi} M \xrightarrow{\eta} M'' \longrightarrow 0$$

è esatta se e solo se per ogni A-modulo N la sequenza

$$0 \longrightarrow Hom_A(M'', N) \xrightarrow{\bar{\eta}} Hom_A(M, N) \xrightarrow{\bar{\phi}} Hom_A(M', N)$$

è esatta.

2.3 Moduli finitamente generati

Siano M un A-modulo, e Q un ideale di A; allora, per ogni $x \in M$, l'insieme

$$Q \cdot x = \{q \cdot x \mid q \in Q\}$$

è un A-sottomodulo di M. Più in generale, per ogni $\emptyset \neq X \subseteq M$, l'insieme

$$Q \cdot X = \{q_1x_1 + \ldots + q_nx_n \mid 1 \leq n \in \mathbb{N},\ q_1, \ldots, q_n \in Q,\ x_1, \ldots, x_n \in X\}$$

è un A-sottomodulo di M; osserviamo che se $X = \{x_1, \ldots, x_t\}$ è finito si ha

$$Q \cdot X = Q \cdot x_1 + \ldots + Q \cdot x_t.$$

In particolare, per ogni $x \in M$, $A \cdot x$ è un A-sottomodulo, detto sottomodulo ciclico di M. Di fatto, se X è un sottoinsieme non vuoto dell'A-modulo M, allora $A \cdot X$ è il minimo A-sottomodulo contenente X (si osservi che, se Q è un ideale di A non è detto che $X \subseteq Q \cdot X$ - vedi anche l'esercizio 21), cioè è il sottomodulo generato da X.

DEFINIZIONE. Sia M un A-modulo.

- M si dice *ciclico* se esiste $x \in M$ tale che $M = A \cdot x$;
- M si dice *finitamente generato* se esistono $x_1, \ldots, x_n \in M$, con $1 \leq n \in \mathbb{N}$, tali che $M = A \cdot x_1 + \cdots + A \cdot x_n$.

ESEMPIO 1. Ogni anello A, come modulo su se stesso, è ciclico; più in generale per ogni ideale I di A il quoziente A/I è un A-modulo ciclico (generato da $1 + I$). Dall'altra parte, gli ideali di A (cioè i sottomoduli di A su se stesso) che sono ciclici sono gli ideali principali.

ESEMPIO 2. Un modulo ciclico su $\mathbb{Z}$ è un gruppo ciclico.

Come sempre, occorre cautela nel farsi ispirare troppo da quel che avviene nei casi basici (gruppi abeliani o spazi vettoriali). Per esempio, ogni sottogruppo di un gruppo ciclico è ciclico, ed ogni sottospazio di uno spazio vettoriale finitamente generato è finitamente generato, mentre esistono moduli ciclici che ammettono sottomoduli che non sono finitamente generati. Un esempio è l'anello dei polinomi a coefficienti nel campo $\mathbb{K}$ su un insieme numerabile di indeterminate: $A = \mathbb{K}[x_1, x_2, \ldots]$; A è ciclico come modulo su se stesso, mentre l'ideale $(x_1, x_2, \ldots)$ è un A-sottomodulo che non è finitamente generato.

ESEMPIO 3. Il gruppo additivo $\mathbb{Q}$ dei numeri razionali è uno $\mathbb{Z}$-modulo, che denotiamo con M, che non è finitamente generato; tuttavia ogni coppia di elementi $a/b, c/d$ di M è 'dipendente' su $\mathbb{Z}$: $b(a/b) - d(c/d) = 0$; più in generale, ogni $\mathbb{Z}$-sottomodulo finitamente generato di M è ciclico (esercizio).

ESEMPIO 4. Siano $\mathbb{K}$ un campo, V uno spazio vettoriale di dimensione finita su $\mathbb{K}$ e $\phi \in End(V)$. Mediante ϕ è un'azione dell'anello dei polinomi $\mathbb{K}[x]$ su V che rende quest'ultimo un $\mathbb{K}[x]$-modulo (esempio 4) della sezione 2.1). L'annullatore di V come $\mathbb{K}[x]$-modulo è l'ideale generato dal polinomio minimo $m_\phi \in \mathbb{K}[x]$ di ϕ. Il Teorema 2.5 della prima parte del corso afferma che, se m_ϕ coincide con il polinomio caratteristico di ϕ, allora esiste $v_0 \in V$ tale che $V = \mathbb{K}[x] \cdot v_0$, ovvero che V è un $\mathbb{K}[x]$-modulo ciclico.

Esercizio 21. Siano M un A-modulo, X un fissato elemento di M e I un ideale di A. Si provi che $x \in I \cdot x$ se e solo se $I \cdot x = A \cdot x$. Si concluda che $A \cdot x$ è il minimo A-sottomodulo di M che contiene x.

Se $M = A \cdot x$ è un A–modulo ciclico, l'applicazione $\pi : A \to M$ definita da $\pi(a) = a \cdot x$, per ogni $a \in A$, è un omomorfismo suriettivo di A-moduli; dunque

$$M \simeq_A A/\ker \pi$$

dove $\ker)\pi) = Ann_A(x)$. Quindi *ogni A-modulo ciclico è isomorfo ad un quoziente di A* (e viceversa, come osservato nell'esempio 1). Per estendere questo tipo di caratterizzazione a moduli finitamente generati, occorre introdurre il concetto di modulo libero.

DEFINIZIONE. Un A-modulo M si dice *libero* se

$$M \simeq_A \bigoplus_{\lambda \in \Lambda} M_\lambda \tag{4}$$

dove Λ è un insieme e, per ogni $\lambda \in \Lambda$, $M_\lambda \simeq_A A$.

Nel caso finitamente generato (cioè l'insieme Λ in (4) è finito) si può dare una definizione più diretta: si definisce induttivamente, per $n \geq 1$, il A-modulo libero A^n ponendo $A^1 = A$ (come A-modulo) e, per $n \geq 1$, $A^{n+1} = A^n \oplus A$ (ovvero, $A^n = A \oplus \cdots \oplus A$, con n copie di A nella somma diretta). A^n si chiama il A-modulo *libero di rango n*.

Proposizione 25. *Sia M un A-modulo finitamente generato. Allora M è isomorfo ad un quoziente di un modulo libero finitamente generato A^n.*

Dimostrazione. Siano, per qualche intero $n \geq 1$, $x_1, \ldots, x_n \in M$ tali che $M = Ax_1 + \ldots + Ax_n$, e sia $\pi : A^n \to M$ l'applicazione definita da

$$\pi(a_1, \ldots, a_n) = a_1x_1 + \ldots + a_nx_n,$$

per ogni $(a_1, \ldots, a_n) \in A^n$. Si verifica facilmente che π è un omomorfismo suriettivo di A-moduli, e dunque $M \simeq_A A^n/\ker(\pi)$ per il Teorema di omomorfismo. □

Teorema 26 (Lemma di Nakayama)**.** *Sia M un A-modulo finitamente generato e* $\mathrm{J} = \mathrm{J}(A)$ *il radicale di Jacobson di A. Allora* $\mathrm{J}M = M \iff M = \{0\}$.

Dimostrazione. Basta ovviamente provare che se $\mathrm{J}M = M$ allora M è il modulo nullo. Supponiamo $M \neq \{0\}$ e sia $x_1, \ldots, x_n$ un insieme minimale di generatori di M come A-modulo. Se, per assurdo, $\mathrm{J}M = M$ si ha in particolare che esistono $a_1, \ldots, a_n \in \mathrm{J}$ tali che $x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_nx_n$, ovvero

$$(1 - a_n)x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}.$$

Ma, per il Lemma 10, $1 - a_n$ è un elemento invertibile di A: se b è il suo inverso, si trova $x_n = ba_1x_1 + \cdots + ba_{n-1}x_{n-1}$, il che contraddice la minimalità dell'insieme di generatori $\{x_1, \ldots, x_n\}$. □

Corollario 27. *Sia M un A-modulo finitamente generato, N un suo sottomodulo, e $\mathrm{J} = \mathrm{J}(A)$ il radicale di Jacobson di A. Se $M = \mathrm{J}M + N$ allora $M = N$.*

Dimostrazione. Si applica il Lemma di Nakayama al A-modulo $\overline{M} = M/N$. Infatti, l'ipotesi $\mathrm{J}M + N = M$ significa $\mathrm{J}(\overline{M}) = \overline{M}$. Dunque $\overline{M} = \{0\}$, ovvero $M = N$. □

Esempio 1. Sia A un anello locale, $\mathfrak{m}$ il suo unico ideale massimale e $\mathbb{K} = A/\mathfrak{m}$ il suo campo residuo. Se $M \neq \{0\}$ è un A-modulo finitamente generato, allora, per il lemma di Nakayama, $\mathfrak{m}M$ è un sottomodulo proprio, e $\mathfrak{m} = Ann_A(M/\mathfrak{m}M)$. Quindi $M/\mathfrak{m}M$ è un modulo per il campo $\mathbb{K} = A/\mathfrak{m}$ e dunque è un $\mathbb{K}$-spazio vettoriale di dimensione finita. Siano $x_1, \ldots, x_n \in M$ tali che $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ è una base di $M/\mathfrak{m}M$ come $\mathbb{K}$-spazio vettoriale, e sia N il sottomodulo di M generato da $\{x_1, \ldots x_n\}$. Allora

$$\frac{N + \mathfrak{m}M}{\mathfrak{m}M} = \frac{M}{\mathfrak{m}M},$$

quindi $N + \mathfrak{m}M = M$ e dunque, per il Corollario 27, $M = N$.

Esempio 2. Sia G un gruppo, $\mathbb{K}$ un campo e $A = \mathbb{K}[G]$ l'anello gruppale associato. Sia $M \neq 0$ un A-modulo; poiché A contiene $\mathbb{K}1_G \simeq \mathbb{K}$ come sottoanello, e $\mathbb{K}1_G \cap Ann_A(M) = \{0\}$, si ha che M è anche un modulo per $\mathbb{K}$, dunque uno spazio vettoriale su $\mathbb{K}$. I moduli per $A = \mathbb{K}[G]$ si chiamano $\mathbb{K}$-rappresentazioni del gruppo G.
Mettiamoci nel caso, esaminato in precedenza, in cui $\mathbb{K}$ è un campo di caratteristica $p > 0$ e G un p-gruppo (abeliano). Allora, come abbiamo visto, $\mathbb{K}[G]$ è un anello locale e il suo radicale di Jacobson è l'ideale aumentante:

$$\mathrm{J} = \mathrm{J}(\mathbb{K}[G]) = \Big\{ \sum_{g \in G} \alpha(g) g \;\Big|\; \sum_{g \in G} \alpha(g) = 0 \Big\}$$

e $\mathbb{K}[G]/\mathrm{J} \simeq \mathbb{K}$. Sia M una $\mathbb{K}$-rappresentazione finitamente generata di G, e supponiamo che sia *semplice* (un modulo $M \neq 0$ si dice *semplice* se $\{0\}$ ed M sono i soli sottomoduli). Ora, per il lemma di Nakayama, $\mathrm{J}M$ è un sottomodulo proprio di M e dunque $\mathrm{J}M = \{0\}$ e, poiché J è un ideale massimale, si ha $\mathrm{J} = Ann_{\mathbb{K}[G]}(M)$ e $M \simeq_{\mathbb{K}[G]} \mathbb{K}[G]/\mathrm{J} \simeq \mathbb{K}$ (il che vuol dire che ogni elemento $1_{\mathbb{K}} g \in G$ agisce come l'identità su M).

Proposizione 28. *Sia M un A-modulo finitamente generato, sia Q un ideale di A e $\phi : M \to M$ un endomorfismo di A-moduli tale che $\phi M \subseteq Q \cdot M$. Allora, in $End_A(M)$, ϕ soddisfa un identità della forma*

$$\phi^n + a_1 \phi^{n-1} + \cdots + a_n = 0,$$

con $a_0, \ldots a_n \in Q$.

Dimostrazione. Sia $x_1, x_2, \ldots, x_n$ un sistema di generatori di M (come A-modulo). Dall'ipotesi $\phi(M) \subseteq I \cdot M$ segue che, per ogni $i = 1, \ldots, n$,

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j,$$

con $a_{ij} \in Q$. Quindi, scrivendo con δ_{ij} il delta di Kronecker, si ha in $End_A(M)$,

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

identità che possiamo riscrivere in forma matriciale (con coefficienti in $End_A(M)$) come $(I\phi - A) \cdot X = 0$, con $A = \big(a_{ij}\big)$, $I = \big(\delta_{ij}\big)$ la matrice identica, e $X = (x_1 \ldots x_n)^T$. Denotando con $C = \big(C_{ij}\big)$ la matrice dei complementi algebrici di $(I\phi - A)$ si ha

$$0 = C(I\phi - A) \cdot X = \det(I\phi - A) I \cdot X,$$

ovvero $\det(I\phi - A)x_i = 0$ per ogni $i = 1, \ldots, n$. Poiché $\{x_1, \ldots, x_n\}$ è un sistema di generatori per M, ciò significa $\det(I\phi - A) = 0 \in End_A(M)$; sviluppando il determinante, si ottiene l'identità cercata. □

NOTA. La Proposizione 28, che tornerà molto utile più avanti, si applica ad esempio per un'altra dimostrazione del Lemma di Nakayama. Infatti sia M un A-modulo finitamente generato tale che $\mathrm{J}(A)M = M$; applicando la Proposizione 28 all'omomorfismo identico si trova che esistono $n \geq 1$ e $a_1, \ldots, a_n \in \mathrm{J}(A)$ tali che, per ogni $x \in M$,

$$0 = x - (a_1 + \ldots + a_n)x = (1_A - (a_1 + \ldots + a_n))x. \tag{5}$$

Per il Lemma 10, $1_A - (a_1 + \ldots + a_n)$ è invertibile in A, dunque da (5) segue $x = 0$.

Esercizio 22. [ex 2.10 in A.M.] Siano A un anello e I un ideale contenuto in $\mathrm{J}(A)$; siano poi M, N due A-moduli con N finitamente generato e sia $\phi : M \to N$ un omomorfismo di A-moduli. Si provi che se l'omomorfismo indotto $M/IM \to N/IN$ è suriettivo allora ϕ è suriettivo.

Esercizio 23. [ex 2.12 in A.M. + altro] Siano A un anello, M un A-modulo finitamente generato e $\phi : M \to A^n$ $(n \geq 1)$ un omomorfismo suriettivo di A-moduli. Si provi che

(1) $K = \ker(\phi)$ è finitamente generato come A-modulo;

(2) $M \simeq_A \ker(\phi) \oplus N$ con N un A-sottomodulo di M e $N \simeq_A A^n$.

Esercizio 24. Sia A un dominio d'integrità che non sia un campo e Q il suo campo delle frazioni. Si provi che, come A-modulo, Q non è finitamente generato.

Esercizio 25. Sia A un anello. Se M è un A-modulo, $M^* = Hom_A(M, A)$ è detto *modulo duale* di M.

(1) Si definisca un omomorfismo naturale di A-moduli $M \to Hom_A(M^*, A)$.

(2) Si provi che se M è un A-modulo libero finitamente generato allora

$$Hom_A(M^*, A) \simeq_A M.$$

2.4 Prodotto tensoriale di moduli

DEFINIZIONE. Sia A un anello. Dati A-moduli M, N, L, un'applicazione $f : M \times N \to L$ si dice A-*bilineare* se per ogni $x \in M$, e per ogni $y \in N$,

- l'applicazione $N \to L$ definita da $y \mapsto f(x, y)$, per ogni $y \in N$, e
- l'applicazione $M \to L$ definita da $x \mapsto f(x, y)$, per ogni $y \in M$,

sono A-lineari.

ESEMPI. 1) Un esempio banale: se A è un anello, la moltiplicazione $A \times A \to A$ è un'applicazione A-bilineare.

2) Se $\mathbb{K}$ è un campo e $n \geq 1$, un prodotto scalare $\mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ è un applicazione $\mathbb{K}$-bilineare. Più in generale, se A è una matrice $n \times n$ su $\mathbb{K}$, la funzione $\mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ definita da $(X, Y) \mapsto XAY^T$ è $\mathbb{K}$-bilineare.

3) Siano A un anello, M un a A-modulo e N un A-sottomodulo di $Hom_A(M, A)$; la funzione $M \times N \to A$ definita da $(x, \phi) \mapsto \phi(x)$ (per ogni $x \in M, \phi \in N$) è A-bilineare.

Un fatto la cui verifica è facile routine, ma che useremo più d'una volta senza dirlo è che se M, N, L, P sono A-moduli e le applicazioni $f : M \times N \to L$ e $g : L \to P$ sono, rispettivamente, A-bilineare e A-lineare, allora $g \circ f : M \times N \to P$ è A-bilineare.

Se M, N e L sono A-moduli, l'insieme $Bil_A(M, N; L)$ di tutte le applicazioni A-bilineari da $M \times N$ in L è naturalmente un A-modulo (definizione e verifiche per esercizio).

ESEMPI. 1) Siano m, n interi positivi e coprimi, e siano $r, s \in \mathbb{Z}$ tali che $rm + sn = 1$. Consideriamo gli $\mathbb{Z}$-moduli $M = \mathbb{Z}/m\mathbb{Z}$ e $N = \mathbb{Z}/n\mathbb{Z}$. Se L è uno $\mathbb{Z}$-modulo (gruppo additivo), e $f : M \times N \to L$ un'applicazione $\mathbb{Z}$-bilineare, allora, per ogni $(x, y) \in M \times N$,

$$\begin{aligned} f(x, y) &= 1 \cdot f(x, y) = (rm + sn)f(x, y) = rmf(x, y) + snf(x, y) = \\ &= rf(mx, y) + sf(x, ny) = rf(0, y) + sf(x, 0) = 0 + 0 = 0; \end{aligned}$$

ovvero, f è la funzione nulla. Quindi $Bil_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}; L) = 0$ per ogni $\mathbb{Z}$-modulo L.

2) Siano M uno $\mathbb{Z}$-modulo e $f : \mathbb{Z} \times \mathbb{Z} \to M$ un'applicazione $\mathbb{Z}$-bilineare. Posto $d = f(1, 1)$ si ha, per ogni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$,

$$f(x, y) = xf(1, y) = xyf(1, 1) = (xy)d.$$

Da ciò si deduce facilmente che $Bil_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z};M) \simeq Hom_{\mathbb{Z}}(\mathbb{Z},M) \simeq_{\mathbb{Z}} M$.

Dati due A-moduli M e N, mediante il loro prodotto tensoriale si vuole, in particolare, trovare un A-modulo T tale che $Bil_A(M,N;L) \simeq_A Hom_A(T,L)$, per ogni A-modulo L. Più precisamente, introduciamo la seguente proprietà universale.

DEFINIZIONE. Dati A-moduli M, N, un *prodotto tensoriale* di M e N è una coppia (T,g), dove T è un A-modulo e $g : M \times N \to T$ un'applicazione A-bilineare, tale che *per ogni A-modulo L ed ogni applicazione A-bilineare $f : M \times N \to L$ esiste una ed un'unica applicazione A-lineare $T \to L$ tale che $f = f' \circ g$* (vedi diagramma).

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & T \\ {\scriptstyle f}\downarrow & \swarrow & \nearrow {\scriptstyle f'} \\ L & & \end{array} \tag{6}$$

Prima di stabilirne l'esistenza, vediamo che un prodotto tensoriale, se esiste, è univocamente individuato a meno di isomorfismo. Supponiamo, infatti, che (T,g) e (P,f) siano due prodotti tensoriali degli A-moduli M e N. Per definizione, esistono allora omomorfismi $f' : T \to P$ e $g' : P \to T$ tali che $f = f' \circ g$ e $g = g' \circ f$. Quindi

$$(g' \circ f') \circ g = g' \circ f = g,$$

il che implica (per la proprietà di unicità nella (6) applicata a $L = T$ e $f = g$) che $g' \circ f'$ è l'identità su T; similmente, si prova che $f' \circ g'$ è l'identità su P. In particolare f' e g' sono biezioni e dunque isomorfismi di A-moduli.

Proviamo ora l'esistenza del prodotto tensoriale di due A-moduli M ed N. Sia $\mathfrak{C}$ l'A-modulo libero generato dagli elementi di $M \times N$. Concretamente, $\mathfrak{C} = A^{(M\times N)}$ è l'A-modulo costituito da tutte le funzioni $M \times N \to A$ quasi ovunque nulle; formalmente, i suoi elementi possono essere descritti da somme finite $\sum_{i=1}^{n} a_i(x_i, y_i)$, con $a_i \in A$ e $(x_i, y_i) \in M \times N$ e le operazioni puntuali del prodotto diretto. Sia $\mathfrak{D}$ il sottomodulo generato da tutti gli elementi dalle seguenti forme:

$$\begin{gathered} (x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y') \\ (ax, y) = a(x, y) \\ (x, ay) = a(x, y) \end{gathered} \tag{7}$$

con $x, x' \in M$, $y, y' \in N$ e $a \in A$.
Poniamo $T = \mathfrak{C}/\mathfrak{D}$, cheè un A-modulo. La funzione chiamata g in (6) è quella naturale:

$$\begin{array}{rccl} \otimes : & M \times N & \to & T \\ & (x, y) & \mapsto & x \otimes y := (x, y)\mathfrak{D} \end{array}$$

Che questa sia A-bilineare segue subito dalla definizione (7) del sottomodulo $\mathfrak{D}$; ad esempio, dalla terza in (7) segue che

$$x \otimes ay = (x, ay)\mathfrak{D} = a(x, y)\mathfrak{D} = a(x \otimes y) = (ax) \otimes y,$$

e così similmente, per ogni $x, x' \in M$ e $y, y' \in N$,

$$(x + x') \otimes y = x \otimes y + x' \otimes y \quad \text{e} \quad x \otimes (y + y') = x \otimes y + x \otimes y'.$$

Accertiamoci quindi che T soddisfi la proprietà universale in (6). Sia L un A-modulo; ogni applicazione $f : M \times N \to L$ si estende in modo naturale ad un'applicazione A-lineare $\tilde{f} : \mathfrak{C} \to L$:

$$\tilde{f}\Big(\sum_{i=1}^{n} a_i(x_i, y_i)\Big) = \sum_{i=1}^{n} a_i f(x_i, y_i).$$

Se inoltre f è A-bilineare, si ha $\mathfrak{D} \leq \ker(\tilde{f})$, quindi $\tilde{f}$ induce un'applicazione A-lineare $f' : T = \mathfrak{C}/\mathfrak{D} \to L$; per ogni $(x, y) \in M \times N$, $f'(x \otimes y) = \tilde{f}(x, y) = f(x, y)$, quindi $f' \circ \otimes = f$, come si voleva concludere.

L'A-modulo T costruito sopra, unico a meno di isomorfismo, si chiama il *prodotto tensoriale* di M e N e si denota con $M \otimes_A N$. Come A-modulo, $M \otimes_A N$ è generato dagli elementi $x \otimes y$, con $x \in M$, $y \in N$; con maggior precisione, se X e Y sono, rispettivamente, sistemi di generatori di M e di N, allora $M \otimes_A N$ è generato dall'insieme degli elementi $x \otimes y$ con $x \in X$ e $y \in Y$. In particolare, il prodotto tensoriale di due A-moduli ciclici è ciclico, ed anche

Proposizione 29. *Il prodotto tensoriale di due A-moduli finitamente generati è un A-modulo finitamente generato.*

Esempi. 1) In termini di prodotto tensoriale, gli esempi a pagina 32 si leggono come:

- se m, n sono interi positivi e coprimi, allora $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$.
- $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Z}$.

2) Se M è un A-modulo, allora per ogni $a \in A$ e $x \in M$, $a \otimes x = a1 \otimes x = 1 \otimes ax$; da ciò segue $A \otimes_A M = \{1 \otimes m \mid m \in M\}$, ed anche $A \otimes_A M \simeq_A M$.
Quindi, in particolare $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$; mentre si ha $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) = 0$ (dire perché); si osservi qui che $\mathbb{Z}$ è un $\mathbb{Z}$-sottomodulo di $\mathbb{Q}$.

Siano M ed N due A-moduli, allora l'applicazione $f : M \times N \to N \otimes_A M$, definita da $(x, y) \mapsto y \otimes x$ è A-bilineare, e dunque esiste ed è unica l'applicazione A-lineare $f' : M \otimes_A N \to N \otimes_A M$ tale che $f' \circ \otimes = f$, ovvero $f'(x \otimes y) = y \otimes x$ per ogni $(x, y) \in M \times N$. Ragionando nell'altro verso si stabilisce, come nelle dimostrazione dell'unicità del prodotto tensoriale, che f' è invertibile e dunque che è un isomorfismo di A-moduli

(che diciamo "canonico"). In modo simile si provano altre istanze di omomorfismi canonici tra prodotti tensoriali di A-moduli (le dimostrazioni mancanti ed anche il rendere esplicito in cosa consista, in ciascun caso, la "canonicità", sono lasciati per esercizio).

Proposizione 30. *Siano A un anello e M, N, L degli A-moduli. Esistono isomorfismi "canonici"*

(1) $M \otimes_A N \simeq N \otimes_A M$;

(2) $A \otimes_A M \simeq_A M$;

(3) $(M \otimes_A N) \otimes_A L \simeq M \otimes_A (N \otimes_A L)$;

(4) $(M \oplus N) \otimes_A L \simeq (M \otimes_A L) \oplus (N \otimes_A L)$.

Dimostrazione. Per il punto (1) vedi sopra; il resto per esercizio. □

Esercizio 26. Sia $\mathbb{K}$ un campo e siano U, V spazi vettoriali su $\mathbb{K}$ di dimensione finita. Si provi che $\dim_{\mathbb{K}}(U \otimes V) = \dim_{\mathbb{K}}(U) \dim_{\mathbb{K}}(V)$. Più in generale, si provi che per ogni anello A e interi positivi $, m$ si ha $A^n \otimes A^m \simeq_A A^{nm}$.

Esercizio 27. Siano M, N, P degli A-moduli; si provi l'esistenza isomorfismi naturali

$$Bil_A(M, N; P) \simeq_A Hom_A(M \otimes N, P) \simeq_A Hom_A(M, Hom_A(N, P)).$$

Estensione degli scalari. Una prima applicazione del prodotto tensoriale riguarda la cosiddetta "estensione degli scalari".
Sia $\phi : A \to B$ un omomorfismo di anelli. Ad ogni B-modulo N si associa allora in modo naturale (tale procedura si chiama *restrizione degli scalari*) un A-modulo ponendo, per ogni $x \in N$ e ogni $a \in A$, $a \cdot x = \phi(a)x$. In particolare, B stesso assume una struttura di A-modulo.
Partendo - al contrario - da un A-modulo M, vogliamo trovare il modo, mediante ϕ, di associarvi un B-modulo: per quanto detto sopra, B è un A-modulo; possiamo quindi considerare $M_B = B \otimes_A M$. Ed è queste che ammette una struttura naturale di B-modulo: per ogni $b, b' \in B$ ed ogni $x \in M$,

$$b(b' \otimes x) = bb' \otimes x$$

il B-modulo M_B è detto ottenuto dall'A-modulo M per *estensione degli scalari*. Infatti, la sua applicazione più diffusa riguarda il caso in cui A sia un sottoanello di B e ϕ l'inclusione identica.

ESEMPIO. Siano $A = \mathbb{Z}[\sqrt{5}]$, $M = (2, \sqrt{5})$ ideale di A, e $\mathbb{K} = \mathbb{Q}[\sqrt{5}]$. Come A-modulo, M non è isomorfo ad A (dato, ad esempio, che M non è un ideale principale), tuttavia $A \otimes_A \mathbb{K} \simeq_A M \otimes_A \mathbb{K} \simeq_A \mathbb{K}$.

Omomorfismi e prodotti tensoriali. Siano $\phi : M \to N$ e $\psi : M' \to N'$ omomorfismi di A-moduli; l'applicazione $f : M \times N \to M' \otimes N'$ definita da $f(x, y) = \phi(x) \otimes \psi(y)$ è A-bilineare, dunque esiste un (unico) omomorfismo di A-moduli

$$\phi \otimes \psi : M \otimes N \to M' \otimes N'$$

tale che $(\phi \otimes \psi)(x \otimes y) = \phi(x) \otimes \psi(y)$, per ogni $x \in M, y \in N$.

Il comportamento del prodotto tensoriale applicato a moduli in sequenze esatte costituisce un'importante argomento, del quale riferiamo una sola semplice (ma utile) osservazione.

Proposizione 31. *Sia A un anello e $N \xrightarrow{\nu} M \xrightarrow{\phi} L \longrightarrow 0$ una sequenza esatta di A-moduli e omomorfismi. Allora, per ogni A-modulo P la sequenza*

$$N \otimes P \xrightarrow{\nu \otimes 1_P} M \otimes P \xrightarrow{\phi \otimes 1_P} L \otimes P \longrightarrow 0$$

è esatta (dove 1_P è la funzione identità su P).

Dimostrazione. Si vede subito (tenendo conto che $L \otimes P$ è il modulo generato dagli elementi $x \otimes a$ con $(x, a) \in L \times P$) che $\phi \otimes 1_P$ è suriettiva.
Sia $K = Im(\nu \otimes 1_P)$ che è un A-sottomodulo di $M \otimes P$. Dalla definizione di $\nu \otimes 1_P$ e dall'esattezza della sequenza di partenza, segue subito $K \leq \ker(\phi \otimes 1_P)$. Vogliamo provare che vale l'uguaglianza. Intanto osserviamo che, in ogni caso, $\phi \otimes 1_P$ induce un A-omomorfismo $\bar{g} : (M \otimes P)/K \to L \otimes P$. Tenendo conto della suriettività di ϕ definiamo una funzione $f : L \times P \to (M \otimes P)/K$ ponendo, per ogni $(\phi(x), b)$ con $x \in M,\ b \in P$, $f(\phi(x), b) = x \otimes b + K$. Questa è ben definita: se $x, x' \in M$ sono tali che $\phi(x) = \phi(x')$, allora $x - x' \in \ker(\phi) = Im(\nu)$, e dunque esiste $y \in N$ per cui

$$x \otimes b + K = (x' + \nu(y)) \otimes b + K = (x' \otimes b + K) + (\nu(y) \otimes b + K) = x' \otimes b + K.$$

Inoltre, f è A-bilineare, quindi produce un omomorfismo $\bar{f} : L \otimes P \to (M \otimes P)/K$. Si ha poi, per ogni $(x, b) \in M \times P$, $\bar{f} \circ \bar{g}(x \otimes b + K) = \bar{f}(g(x) \otimes b) = x \otimes b + K$. siccome $(M \otimes P)/K$ è generato dagli elementi del tipo $x \otimes b + K$, si conclude che $\bar{f} \circ \bar{g}$ è l'identità. Da ciò segue $\ker(\phi \otimes 1_p) \leq K$, completando la dimostrazione. □

ESEMPIO. Sia $\mu : \mathbb{Z} \to \mathbb{Z}$ la moltiplicazione per 2 e sia $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ la riduzione modulo 2. Allora la sequenza $0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z}$ è esatta; mentre tensorizzando con

$P = \mathbb{Z}/2\mathbb{Z}$ (come Z-modulo) si ottiene $0 \longrightarrow \mathbb{Z} \otimes P \xrightarrow{\mu\otimes 1} \mathbb{Z} \otimes P \xrightarrow{\pi\otimes 1} \mathbb{Z}/2\mathbb{Z} \otimes P$, che non è una sequenza esatta, dato che, ad esempio, $(\mu \otimes 1)(1 \otimes 1) = 2 \otimes 1 = 1 \otimes 2 = 0$.

Semplici applicazioni della Proposizione 31 nei prossimi due esercizi.

Esercizio 28. [ex 2.2 in A.M.] 1) Sia A un anello. Siano I un ideale di A e M un A–modulo; si provi che $(A/I) \otimes_A M \simeq_A M/(I \cdot M)$.

2) Siano I, J ideali propri dell'anello A; si provi che $(A/I) \otimes_A (A/J) \simeq_A A/(I + J)$.

Esercizio 29. [ex 2.3 in A.M.] Sia A un anello locale e siano M, N A-moduli finitamente generati tali che $M \otimes_A N = 0$. Si provi che $M = 0$ oppure $N = 0$.

Esercizio 30. [Proposizioni 2.16 e 2.17 in A.M.] Sia $\phi : A \to B$ omomorfismo di anelli.

(1) Se B ed N sono finitamente generati come, rispettivamente, A-modulo e B-modulo, allora N_A è finitamente generato come A-modulo.

(2) Se M è un A-modulo finitamente generato, allora M_B è un B-modulo finitamente generato.

Soluzioni di alcuni esercizi.

Esercizio 16 – Soluzione. L'isomorfismo cercato è dato dall'applicazione ottenuta ponendo $\phi \mapsto \phi(1_A)$, per ogni $\phi \in Hom_A(A, M)$. ∎

Esercizio 22 – Soluzione. Sia $L = \mathrm{Im}(\phi)$, L è un sottomodulo di N. Ora, l'omomorfismo indotto $\overline{\phi} : M/IM \to N/IN$ è definito da $\overline{\phi}(x + IM) = \phi(x) + IN$, per ogni $x \in M$. Se $\overline{\phi}$ è suriettivo risulta $N = L + IN$. Poiché N è finitamente generato e $I \subseteq \mathrm{J}(A)$, per il Corollario 27 si conclude che $L = N$. ∎

Esercizio 23 – Soluzione. Sia $e_1, \ldots, e_n$ la base naturale di A^n ($e_1 = (1, 0, \ldots, 0)$, etc.) e per ogni $1 \leq i \leq n$ sia $x_i \in M$ tale che $\phi(x_i) = e_i$. Sia $N = Ax_1 + \cdots + Ax_n$ il sottomodulo di M generato da $\{x_1, \ldots, x_n\}$ e sia $K = \ker(\phi)$. Ora $\phi(N) = A^n$, quindi per ogni $x \in M$ esiste $u \in N$ con $\phi(x) = \phi(u)$ e dunque $x = u + (x - u) \in N + K$. Dunque $M = N + K$. Sia $y = a_1x_1 + \cdots + a_nx_n \in N \cap K$, allora

$$0 = \phi(y) = a_1\phi(x_1) + \cdots + a_n\phi(x_n) = a_1e_1 + \cdots + a_ne_n = (a_1, \ldots a_n),$$

e dunque $y = 0$. Quindi, $N \cap K = \{0\}$. Dunque $M \simeq_A N \oplus K$, che è il punto (2); il punto (1) segue subito, infatti $K \simeq_A M/N$ è finitamente generato. ∎

Esercizio 28 – Soluzione. Applicando la Proposizione 31 al prodotto tensoriale per M della sequenza esatta $I \to A \to A/I \to 0$, dove ι è l'inclusione identica e π la proiezione canonica, si ottiene la sequenza esatta

$$I \otimes M \xrightarrow{\iota\otimes 1} A \otimes M \xrightarrow{\pi\otimes 1} A/I \otimes M \longrightarrow 0.$$

Osservando che $I \otimes M \simeq I \cdot M$, $A \otimes M \simeq M$ e che l'applicazione $\iota \otimes 1$ è l'inclusione identica del primo nel secondo, si ha l'enunciato 1).
Il punto 2) segue da 1), osservando che, se I, J sono ideali di A allora, come A-moduli,

$$I \cdot (A/J) = (AI + J)/J = (I + J)/J,$$

ed applicando quindi il terzo teorema di omomorfismo (Proposizione 24 (2)). ∎

Esercizio 29 – Soluzione. Sia $\mathfrak{m}$ l'unico ideale massimale di A e sia $\mathbb{K} = A/\mathfrak{m}$ il campo residuo. Se M è un A-modulo allora, per l'esercizio 28, $M \otimes_A \mathbb{K} \simeq_A M/\mathfrak{m}M$ che è un $\mathbb{K}$-spazio vettoriale. Si osservi poi che per A-moduli M, N si ha che $M/\mathfrak{m}M \otimes_A N/\mathfrak{m}N$ è uguale, come $\mathbb{K}$-spazio vettoriale a $M/\mathfrak{m}M \otimes_{\mathbb{K}} N/\mathfrak{m}N$.
Dalla Proposizione 30 si ottiene quindi,

$$0 = (M \otimes_A N) \otimes_A \mathbb{K} = (M \otimes_A \mathbb{K}) \otimes_A (N \otimes_A \mathbb{K}) \simeq_{\mathbb{K}} (M/\mathfrak{m}M) \otimes_{\mathbb{K}} (N/\mathfrak{m}N).$$

Dunque (ad esempio per l'esercizio 26) $M/\mathfrak{m}M = 0$ oppure $N/\mathfrak{m}N = 0$, da cui segue, per il Lemma di Nakayama, $M = 0$ oppure $N = 0$. ∎

3 Anelli noetheriani e artiniani

[questa parte è una riduzone dei capitoli 6 e 7 di A.M.]

3.1 Moduli e anelli Noetheriani.

DEFINIZIONE. Si dice che un insieme parzialmente ordinato soddisfa la *proprietà di massimo* se ogni suo sottoinsieme non vuoto ha un elemento massimale.

Proposizione 32. *Sia $(P, \leq)$ un insieme parzialmente ordinato. Le seguenti condizioni sono equivalenti:*

i) ogni successione $x_1, x_2, \ldots$ di elementi di P con $x_1 \leq x_2 \leq \ldots$ [si chiama catena ascendente *in $(P, \leq)$] è stazionaria, ovvero esiste $n \geq 1$ tale che $x_n = x_{n+i}$ per ogni $i \geq 0$;*

ii) $(P, \leq)$ soddisfa la proprietà di massimo.

La proprietà *i)* è chiamata condizione sulle catene ascendenti ed abbreviata in a.c.c. ("ascending chain condition").

Dimostrazione. i) $\Rightarrow$ *ii)*. Supponiamo esista un sottoinsieme $\emptyset \neq Q \subseteq P$ privo di elementi massimali. Allora per ogni $x_1 \in Q$ esiste $x_2 \in Q$ con $x_1 < x_2$; si procede quindi induttivamente, trovando una catena ascendente di elementi di Q (e quindi di P) che non è stazionaria.
i) $\Rightarrow$ *ii)*. Se $(P, \leq)$ soddisfa la proprietà di massimo e $x_1 \leq x_2 \leq \ldots$, allora $Q = \{x_1, x_2, \ldots\}$ ha un elemento massimale x_n che, essendo Q una catena, ne è anche il massimo, e dunque $x_{n+i} = x_n$ per ogni $i \geq 0$. □

Ad esempio, sia P l'insieme degli interi positivi la cui fattorizzazione in primi contiene al più 5 fattori (si conta anche la molteplicità); quando ordinato per divisibilità, P soddisfa la proprietà di massimo, mentre non la soddisfa se ordinato secondo l'ordine naturale degli interi. Ma un esempio più significativo, dal nostro punto di vista, è quello dell'insieme di tutti gli ideali di un dominio a ideali principali, ordinato per inclusione: da quanto studiato nel corso di Algebra I, sappiamo in tale insieme le catene ascendenti sono stazionarie, e quindi esso soddisfa la proprietà di massimo. Ed è proprio questo caso ciò che ci si propone di ampliare introducendo il concetto di anello Noetheriano.

DEFINIZIONE. (1) Un A-modulo M si dice *Noetheriano* (da Emmy Noether) se l'insieme dei sottomoduli ordinato per inclusione, soddisfa la proprietà di massimo (oppure quella delle catene ascendenti secondo il punto i) della Proposizione precedente)).

(2) Un anello A si dice *Neotheriano* se A è tale come A-modulo; ovvero se l'insieme degli ideali di A, ordinato per inclusione, soddisfa la proprietà di massimo.

ESEMPI. • I campi sono ovviamente anelli Noetheriani. Di fatto, come osservato, ogni dominio a ideali principali (come l'anello $\mathbb{Z}$ o l'anello dei polinomi $\mathbb{K}[x]$ a coefficienti su un campo) è un anello Noetheriano.

• Ogni gruppo abeliano finito è uno $\mathbb{Z}$-modulo Noetheriano.

• Se $\mathbb{K}$ è un campo, un $\mathbb{K}$-modulo è uno $\mathbb{K}$-spazio vettoriale V, e l'insieme dei suoi sottomoduli è quello dei sottospazi. Si conclude quindi che V è Noetheriano (come $\mathbb{K}$-modulo) se e soltanto se $\dim(V)$ è finita.

Proposizione 33. (1) *Sia* $0 \longrightarrow N \xrightarrow{\nu} M \xrightarrow{\phi} L \longrightarrow 0$ *una sequenza esatta di A-moduli. Allora, M è Noetheriano se e solo se N e L sono Noetheriani.*

(2) *Se $M_1, \ldots, M_n$ sono A-moduli Noetheriani; allora $\bigoplus_{i=1}^n M_i$ è Noetheriano.*

Dimostrazione. (1) ($\Rightarrow$) Sia M Noetheriano. Sia $\mathcal{Q}$ un insieme non vuoto di sottomoduli di N. Allora $\{\nu(U) \mid U \in \mathcal{Q}\}$ è un insieme di sottomoduli di M e dunque ha un elemento massimale $\nu(U')$. Poiché ν è iniettiva, $U' = \nu^{-1}(\nu(U')$ e quindi U' è un elemento massimale in $\mathcal{Q}$. Questo prova che N è un A-modulo Noetheriano.
Similmente, se $\mathcal{M}$ è un insieme non vuoto di sottomoduli di L, $\{\phi^{-1}V \mid V \in \mathcal{M}\}$ è un insieme di sottomoduli di M ed ammette un massimo $\phi^{-1}(V')$. Poiché ϕ è suriettiva, si conclude che $V' = \phi(\phi^{-1}(V'))$ è un elemento massimale in $\mathcal{M}$. Dunque L è un A-modulo Noetheriano.

($\Leftarrow$) Supponiamo che N e L siano Noetheriani, e sia $K = \mathrm{Im}(\nu) = \ker(\phi)$. Osserviamo che K è un sottomodulo, $K \simeq_A N$ e $M/K \simeq_A L$; quindi, come A-moduli, sia K che M/K sono Noetheriani. Sia $\mathcal{Q}$ un insieme non vuoto di sottomoduli di M. Allora, poiché M/K è Noetheriano esiste $U' \in \mathcal{Q}$ tale che $(U'+K)/K$ è massimale nell'insieme dei sottomoduli $\{(U+K)/K \mid U \in \mathcal{Q}\}$ di M/K. Ma anche l'insieme $\{U \cap K \mid U \in \mathcal{Q},\ U+K = U'+K\}$ è un insieme non vuoto di sottomoduli di K dunque ha un elemento massimale $U^* \cap K$. Ora, $U^* \in \mathcal{Q}$, e se $U^* \subseteq U \in \mathcal{Q}$, allora $U' + K = U^* + K \subseteq U + K$, dunque $U + K = U^* + K = U' + K$ e pertanto $U \cap K = U^* \cap K$. Quindi (poiché $U^* \subseteq U$),

$$U = (U+K) \cap U = (U^*+K) \cap U = U^* + (U \cap K) = U^* + (U^* \cap K) = U^*.$$

Dunque U^* è un elemento massimale di $\mathcal{Q}$, e questo prova che M è Noetheriano.

(2) Per ogni $n \geq 2$, c'è una sequenza esatta naturale di A-moduli

$$0 \longrightarrow \bigoplus_{i=1}^{n-1} M_i \xrightarrow{\nu} \bigoplus_{i=1}^{n} M_i \xrightarrow{\phi} M_n \longrightarrow 0$$

[per ogni n-upla $x_1, \ldots, x_n$, con $x_i \in M_i$, si pone $\nu(x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, 0)$ e $\phi(x_1, \ldots, x_n) = x_n$]. L'affermazione segue, argomentando per induzione su n, come caso particolare del punto (1). □

Il "solo se" al punto (1) dice, in sostanza, che *sottomoduli e quozienti di un modulo Noetheriano sono Noetheriani*; in particolare se $\phi : M \to N$ è un omomorfismo suriettivo di A-moduli e M è Noetheriano, allora N è Noetheriano. Applicato agli anelli si ha

Corollario 34. *Sia I un ideale dell anello Noetheriano A; allora A/I è un anello Noetheriano.*

Un'altra semplice ma fondamentale conseguenza è il seguente fatto.

Corollario 35. *Sia A un anello Noetheriano; allora ogni A-modulo finitamente generato è Noetheriano.*

Dimostrazione. Sia M un A-modulo finitamente generato, con A anello Noetheriano. Allora, per la Proposizione 25, M è isomorfo (come A-modulo) ad un quoziente di un modulo libero finitamente generato A^n. Per il punto (2) della Proposizione 33, A^n è Noetheriano, quindi M è Noetheriano per quanto osservato (punto (1) di 33). □

Vediamo ora una caratterizzazione dei moduli (e anelli) Noetheriani che è una delle ragioni del loro successo.

Proposizione 36. *Un A-modulo M è Noetheriano se e solo se ogni sottomodulo di M è finitamente generato.*

Dimostrazione. Sia M Noetheriano e N un suo sottomodulo. Denotiamo con Σ l'insieme di tutti i sottomoduli finitamente generati di N; tale insieme contiene il modulo nullo $\{0\}$, dunque non è vuoto e pertanto ammette un elemento massimale J. Sia $x \in N$, allora $J+Ax$ è un sottomodulo finitamente generato di N, cioè $J+Ax \in \Sigma$, e $J \subseteq J+Ax$. Dunque, per la massimalità di J in Σ, $J + Ax = J$ e pertanto $x \in J$. Questo prova che $N = J$ è finitamente generato.
Viceversa, supponiamo che ogni sottomodulo di M sia finitamente generato. Sia $N_1 \subseteq N_2 \subseteq \ldots$ una catena ascendente di sottomoduli di M, e $N = \bigcup_{i \geq 1} N_i$. In quanto sottomodulo di M, N è finitamente generato; e se $x_1, \ldots x_k$ è un sistema finito di generatori di N, esiste $n \geq 1$ tale che $\{x_1, \ldots, x_k\} \subseteq N_n$. Ma allora

$$N = Ax_1 + \cdots + Ax_k \subseteq N_n;$$

dunque $N_n = N$, e la catena di sottomoduli è stazionaria in N_n. □

Così, ad esempio, un gruppo abeliano (uno $\mathbb{Z}$-modulo) è Noetheriano se e solo se è finitamente generato (quindi in particolare ogni sottogruppo di un gruppo abeliano finitamente generato è finitamente generato).

Corollario 37. *Un anello è Noetheriano se e solo se ogni suo ideale è un ideale finitamente generato.*

ESEMPIO. Sia $\mathbb{K}$ un campo; l'anello $A = \mathbb{K}[x_1, x_2, \ldots]$ dei polinomi a coefficienti in $\mathbb{K}$ su un'infinità numerabile di indeterminate non è Noetheriano: ad esempio, infatti, la catena di ideali $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots$ non è stazionaria. Come modulo su se stesso A è ciclico, ma il sottomodulo, cioè l'ideale, $(x_1, x_2, \ldots)$ non è finitamente generato come A–modulo. Osserviamo inoltre che A è un dominio d'integrità e dunque si può immergere (come sottoanello) nel suo campo delle frazioni; quindi sottoanelli di un campo non sono necessariamente anelli Noetheriani.

Teorema 38 (Teorema della Base di Hilbert)**.** *Se A è un anello Noetheriano allora $A[x]$ è un anello Noetheriano.*

Dimostrazione. Sia $\mathfrak{J}$ un ideale di $A[x]$. Allora, come si verifica facilmente, l'insieme J dei termini direttivi degli elementi di $\mathfrak{J}$ è un ideale di A (0 è il coefficiente direttivo del polinomio nullo), il quale, poichè A è Noeteriano, è finitamente generato. Assunto $\mathfrak{J} \neq 0$, sia $\{a_1, \ldots, a_n\}$ un sistema di generatori (tutti $\neq 0$) di J e, per ogni $i = 1, \ldots, n$, sia $f_i \in \mathfrak{J}$ tale che a_i è il coefficiente direttivo di f_i. Sia $\mathfrak{J}'$ l'ideale di $A[x]$ generato da $\{f_1, \ldots, , f_n\}$ (quindi, $\mathfrak{J}' \subseteq \mathfrak{J}$), sia, per $0 \leq i \leq n$, $r_i = \deg f_i$ e poniamo $r = \max\{r_i \mid 0 \leq i \leq n\}$.
Sia M l'insieme dei polinomi in $A[x]$ di grado al più $r-1$, M non è un ideale di $A[x]$ ma è un A-modulo che è generato (come A-modulo) da $1, x, \ldots, x^{r-1}$. Proviamo che

$$\mathfrak{J} = (M \cap \mathfrak{J}) + \mathfrak{J}', \tag{8}$$

Sia $f \in \mathfrak{J}$; mostriamo, per induzione sul grado m di f, che $f \in (M \cap \mathfrak{J}) + \mathfrak{J}'$.
Se $m < r$ (il caso si verifica almeno per $f = 0$) allora $f \in M \cap \mathfrak{J}$. Sia quindi $m \geq r$, ed assumiamo di aver provato la cosa per polinomi di grado inferiore. Sia $a \in J$ il coefficiente direttivo di f; allora $a = \sum_{i=1}^{n} u_i a_i$ con $u_1, \ldots, u_n \in A$. Consideriamo

$$g = \sum_{i=1}^{n} u_i f_i x^{m-r_i} \in \mathfrak{J}'$$

allora $f - g \in f + \mathfrak{J}' \subseteq \mathfrak{J}$ e $\deg(f-g) < m$. Per ipotesi induttiva $f - g = f' + g'$ con $f' \in M \cap \mathfrak{J}$ e $g' \in \mathfrak{J}'$, da cui $f = f' + (g' + g) \in (M \cap \mathfrak{J}) + \mathfrak{J}'$, come si voleva.
Quindi $\mathfrak{J} \subseteq (M \cap \mathfrak{J}) + \mathfrak{J}'$, e poiché l'inclusione inversa è ovvia si ha la (8).
Ora, per il Corollario 35, M è un A-modulo Noetheriano, dunque $M \cap \mathfrak{J}$ è un A-modulo finitamente generato per la Proposizione 36. Se $g_1, \ldots, g_k$ è un insieme di generatori di $M \cap \mathfrak{J}$ come A-modulo, da (8) segue che $g_1, \ldots, g_k, f_1, \ldots, f_n$ è un sistema di generatori di $\mathfrak{J}$ come $A[x]$-modulo (cioè come ideale di $A[x]$).
Questo prova che che ogni ideale di $A[x]$ è finitamente generato e dunque, per il Corollario 37, che $A[x]$ è un anello Noetheriano. □

Corollario 39. *Sia A un anello Noetheriano e $1 \leq n \in \mathbb{N}$; allora $A[x_1, \ldots, x_n]$ è Noetheriano.*

ESEMPIO. Come sappiamo dal corso di Algebra I, il dominio $A = \mathbb{Z}[\sqrt{-5}]$ non è a fattorizzazione unica; tuttavia, A è isomorfo ad un quoziente dell'anello $\mathbb{Z}[x]$ che, per il Teorema 38, è Noetheriano, quindi A è Noetheriano.

Vediamo un'altra proprietà generale, semplice ma rilevante, degli anelli noetheriani.

Proposizione 40. *Sia I un ideale dell'anello noetheriano A; allora esiste $n \geq 1$ tale che $(\sqrt{I})^n \subseteq I$.*

Dimostrazione. Poiché A/I è un anello noetheriano, passando al quoziente possiamo limitarci a provare l'affermazione nel caso $I = (0)$, ovvero che in un anello noetheriano A il nil-radicale $N = \mathfrak{N}(A)$ è nilpotente. Infatti, per noetherianità, esistono $x_1, \ldots, x_m \in N$ tali che $N = (x_1, \ldots, x_m)$; proviamo per induzione su m che esiste $n \geq 1$ tale che $N^n = (0)$. Se $m = 1$ la cosa è ovvia dato che x_1 è un elemento nilpotente; sia $m \geq 2$, $J = (x_m)$ e $t \in \mathbb{N}$ con $x_m^t = 0$. Poiché A/J è noetheriano, per ipotesi induttiva esiste $\ell \geq 1$ tale che $\{J\} = (0_{A/J}) = (N/J)^\ell = N^\ell J/J$, cioè $N^\ell \subseteq J$. Ma allora $N^{\ell t} \subseteq J^t = (0)$. □

Segue un po' di esercizi.

Esercizio 31. [ex 6.1 in A.M.] Sia M un A-modulo Noetheriano, e $\phi : M \to M$ un omomorfismo di A-moduli. Si provi che se ϕ è suriettivo allora è un isomorfismo.

Esercizio 32. [ex 6.4 in A.M.] Sia M un A-modulo Noetheriano, e $\mathfrak{J} = Ann_A(M)$. Si provi che $A/\mathfrak{J}$ è un anello Noetheriano.

Esercizio 33. [ex 7.1 in A.M.] Sia Σ l'insieme degli ideali non finitamente generati di un anello non Noetheriano A. Si provi che Σ, ordinato per inclusione, ammette elementi massimali e che gli elementi massimali di Σ sono ideali primi. Se ne deduce che un anello è Noetheriano se ogni suo ideale primo è fintamente generato (un risultato di I. S. Cohen).

Esercizio 34. [ex 7.2 in A.M.] Sia A un anello Noetheriano. Si provi che un elemento $f = \sum_{n \geq 0} a_n x^n$ di $A[[x]]$ è nilpotente se e solo se ogni coefficiente a_i è un elemento nilpotente di A. [Sugg. usare la Proposizione 40.]

ESEMPIO. [Remark pag.81 in A.M.] Verifichiamo la seguente affermazione: *se A è un anello Noetheriano allora l'anello $A[[x]]$ delle serie formali su A è Noetheriano.*

Se $0 \neq f = \sum_{i\in\mathbb{N}} a_i x^i \in A[[x]]$, chiamiamo *primo termine* di f il coefficiente a_n tale che $a_n \neq 0$ mentre $a_i = 0$ per ogni $i \leq n$, e diciamo che n è il grado di f; mentre se $f = 0$ diciamo che il suo primo termine è 0.
Sia $\mathfrak{J}$ un ideale di $A[[x]]$, e assumiamo $\mathfrak{J} \neq (0)$. Si verifica facilmente che l'insieme dei primi termini degli elementi di $\mathfrak{J}$ è un ideale J di A.
Sia $0 \neq f_1 \in \mathfrak{J}$ di grado minimo e a_1 il suo primo termine. Se $(a_1) \neq J$, sia $f_2 \in \mathfrak{J}$ di grado minimo tale che il suo primo termine a_2 non appartiene a (a_1). Così proseguendo si definisce una sequenza $f_1, f_2, \ldots$ di elementi di $\mathfrak{J}$ tale che, se a_i denota il primo termine di f_i, per ogni indice $i \geq 1$, f_{i+1} è un elemento di $\mathfrak{J}$ di grado minimo tale che il suo primo termine a_{i+1} non appartiene all'ideale $(a_1, \ldots, a_i)$ di A. Per ogni $i \geq 1$, denotiamo con d_i il grado di f_i ed osserviamo che, per costruzione, $d_{i+1} \geq d_i$ per ogni i. Ora, poiché A è Noetheriano, la catena di ideali

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

è necessariamente finita; cioè esiste $n \geq 1$ tale che $J = (a_1, a_2, \ldots, a_n)$.
Sia $\mathfrak{J}'$ l'ideale di $A[[x]]$ generato da $f_1, \ldots, f_n$; proveremo che $\mathfrak{J}' = \mathfrak{J}$. Poiché $\mathfrak{J}' \subseteq \mathfrak{J}$ per costruzione, proviamo l'inclusione inversa.
Sia $0 \neq g \in \mathfrak{J}$, d il suo grado e $a \in A$ il suo primo termine. Poiché $a \in J$ esistono $u_1, \ldots, u_n \in A$ tali che

$$a = \sum_{i=1}^{n} u_i a_i. \tag{9}$$

– Sia $d \geq d_n$. Poniamo

$$g_1 = \sum_{i=1}^{n} u_{1,i} x^{d-d_i} f_i \in \mathfrak{J}'$$

con $u_{1,i} = u_i$ per ogni $1 \leq i \leq n$. Allora, $g - g_1 \in \mathfrak{J}$ ed ha grado $\geq d + 1$.
Per $k \geq 1$, supponiamo di aver definito, per ogni $i = 1, \ldots, k$, elementi $g_i \in \mathfrak{J}'$ tali che il grado di

$$g - \sum_{i=1}^{k} g_i$$

è almeno $d + k$. Sia b il coefficiente di grado $d + k$ di tale serie; allora $b \in J$ (può anche essere $b = 0$) ed esistono $u_{k+1,1}, \ldots u_{k+1,n} \in A$ tali che $b = \sum_{i=1}^{n} u_{k+1,i} a_i$; poniamo

$$g_{k+1} = \sum_{i=1}^{n} u_{k+1,1} x^{d+k-d_i} f_i.$$

Allora, $g_{k+1} \in \mathfrak{J}'$, ed il grado di $g - \sum_{i=1}^{k+1} g_i$ è almeno $d + k + 1$. In questo modo, si ottiene una successione $g_1, g_2, \ldots$ di elementi di $\mathfrak{J}'$ con $grado(g_{i+1}) > grado(g_i)$ per

ogni $i \geq 1$. Questo consente di poter considerare la somma di tutte: se per ogni $i \geq 1$, $g_i = \sum_{j\in\mathbb{N}} b_{j,i}x^j$, allora $b_{j,i} = 0$ se $j \leq i$; si ha

$$\sum_{i=1}^{\infty} g_i = \sum_{j\geq 1} \Big(\sum_{i=1}^{j} b_{j,i} \Big) x^i \in A[[x]].$$

Ma, per costruzione,

$$g = \sum_{i=1}^{\infty} g_i = \sum_{i=1}^{\infty} \Big(\sum_{j=1}^{n} u_{i,j} x^{d+i-1-d_j} f_j \Big) = \sum_{j=1}^{n} \Big(\sum_{i=1}^{\infty} u_{i,j} x^{d-d_j-1+i} \Big) f_j \in \mathfrak{J}'.$$

– Sia ora $d \leq d_n$. Allora c'è un minimo $1 \leq m \leq n$ tale che $a \in (a_1, \ldots, a_m)$ (ideale di A). Osserviamo che, per la scelta di f_m, $d \geq d_m$ e procediamo per induzione su $d_n - d$ (il caso $d_n - d = 0$ rientra tra quelli precedenti). Siano $u_i \in A$ come definiti in (9), allora

$$h = g - \sum_{i=1}^{m} u_i x^{d-d_m} f_i$$

appartiene a $\mathfrak{J}$ e $grado(h) > d$. Per l'ipotesi induttiva, o per il caso precedente, $h \in \mathfrak{J}'$ e dunque $g = h + \sum_{i=1}^{m} u_i x^{d-d_m} f_i \in \mathfrak{J}'$, così completando la dimostrazione.

3.2 Moduli e anelli artiniani.

Un insieme parzialmente ordinato $(P, \leq)$ soddisfa la condizione sulle catene discendenti [d.c.c.] se P dotato dell'ordine opposto $\geq$ (cioè, per ogni $x, y \in P$, $x \geq y \;\Leftrightarrow\; y \leq x$) soddisfa a.c.c., ovvero se ogni successione $x_1, x_2, \ldots$ di elementi di P con $x_1 \geq x_2 \geq \ldots$ [catena discendente] è *stazionaria*, cioè esiste $n \geq 1$ tale che $x_n = x_{n+i}$ per ogni $i \geq 0$. La Proposizione 32, applicata all'ordinamento opposto su P, diventa

Proposizione 41. *Sia $(P, \leq)$ un insieme parzialmente ordinato. Le seguenti condizioni sono equivalenti:*

i) $(P, \leq)$ soddisfa la condizione sulle catene discendenti;

ii) $(P, \leq)$ soddisfa la proprietà di minimo: ovvero ogni sottoinsieme non vuoto di P ammette un elemento minimale.

Definizione. Un A-modulo M si dice *Artiniano* (da Emil Artin) se l'insieme dei sottomoduli di M, ordinato per inclusione, soddisfa la proprietà delle catene discendenti (ovvero quella di minimo). Un anello A si dice *Artiniano* se A è tale come A-modulo; ovvero se l'insieme degli ideali di A, ordinato per inclusione, soddisfa la proprietà di minimo.

ESEMPI. 1. Ogni modulo finito è Artiniano; in particolare ogni gruppo abeliano finito è uno $\mathbb{Z}$-modulo Artiniano.

2. I campi sono anelli Artiniani. Più in generale, se $\mathbb{K}$ è un campo, un $\mathbb{K}$-modulo (cioè un $\mathbb{K}$-spazio vettoriale) è Artiniano se e soltanto se $\dim(V)$ è finita.

3. Sia p un numero primo. Per ogni $n \in \mathbb{N}$ sia $U_{p,n} = \{z \in \mathbb{C} \mid z^{p^n} = 1\}$ il gruppo moltiplicativo delle radice p^n-esime dell'unità, e poniamo

$$U_p = \bigcup_{n\in\mathbb{N}} U_{p,n}.$$

U_p è un gruppo abeliano moltiplicativo e si dimostra (esercizio) che i soli sottogruppi propri di U_p sono gli $U_{p,n}$ al variare di $n \in \mathbb{N}$. Questo implica che U_p è uno $\mathbb{Z}$-modulo artiniano ma non noetheriano.

NOTA. Si può dimostrare che un gruppo abeliano G è artiniano se e solo se esiste un numero finito di primi $p_1, \ldots, p_n$ (non necessariamente distinti) ed un gruppo finito F tali che $G \simeq U_{p_1} \oplus \cdots \oplus U_{p_n} \oplus F$.

Mediante la stessa dimostrazione della Proposizione 33, applicata a catene discendenti invece che ascendenti, si provano le affermazioni seguenti ed i conseguenti Corollari.

Proposizione 42. (1) *Sia* $0 \longrightarrow N \xrightarrow{\nu} M \xrightarrow{\phi} L \longrightarrow 0$ *una sequenza esatta di A-moduli. Allora, M è Artiniano se e solo se N e L sono Artiniani.*

(2) *Se $M_1, \ldots, M_n$ sono A-moduli Artiniani; allora $\bigoplus_{i=1}^n M_i$ è Artiniano.*

Corollario 43. *Sia I un ideale dell'anello Artiniano A; allora l'anello A/I è Artiniano.*

Corollario 44. *Sia A un anello Artiniano; allora ogni A-modulo finitamente generato è Artiniano.*

Non esiste per moduli artiniani una caratterizzazione analoga alla Proposizione 36 per quelli noetheriani. Tuttavia, soprattutto per quel che riguarda gli anelli, la teoria nel caso artiniano è particolarmente semplice.

Lemma 45. *Sia $A \neq 0$ un anello Artiniano; allora*

(1) *se A è un dominio d'integrità A è un campo;*

(2) *ogni ideale primo di A è massimale;*

(3) *l'insieme degli ideali massimali di A è finito.*

Dimostrazione. (1) Sia A un dominio d'integrità e $0 \neq x \in A$. Poiché A è Artiniano, la catena discendente di ideali $(x) \supseteq (x^2) \supseteq \ldots$ ha un minimo, cioè esiste $n \geq 1$ tale che

$(x^{n+1}) = (x^n)$. Quindi $x^n = x^{n+1}y = x^n(xy)$ per qualche $y \in A$ e, per cancellazione (vale nei domini d'integrità), $1 = xy$.

(2) Sia P un ideale primo di A; allora per il Corollario 44 ed il punto (1), A/P è un campo, dunque P è massimale.

(3) Sia Σ l'insieme degli ideali di A che sono intersezione di un numero finito di ideali massimali. Per la proprietà di minimo Σ ha un elemento minimale J (chiaramente, J coincide con il radicale di Jacobson di A); siano $M_1, \ldots, M_n$ ideali massimali distinti di A con $J = M_1 \cap \ldots \cap M_n$. Sia M un ideale massimale di A, allora $J \cap M \in \Sigma$ e dunque $M \supseteq J$; Per il punto (2) del Lemma 4, $M = M_i$ per qualche $1 \leq i \leq n$. □

Proposizione 46. *Sia A un anello Artiniano; allora $\mathfrak{N}(A) = \mathrm{J}(A)$ e $\mathfrak{N}(A)$ è nilpotente.*

Dimostrazione. L'identità $\mathrm{J}(A) = \mathfrak{N}(A)$ segue immediatamente dal punto (2) del Lemma 45. Ora, per la proprietà delle catene discendenti esiste $n \geq 1$ tale che $\mathfrak{N}(A)^n = \mathfrak{N}(A)^{n+i}$ per ogni $i \geq 1$. Sia $N = \mathfrak{N}(A)^n$ e supponiamo $N \neq 0$. Sia Σ l'insieme degli ideali I di A tali che $NI \neq 0$: Σ non è vuoto, perché $N \in \Sigma$, e dunque ammette un elemento minimale K. Allora, esiste $x \in K$ tale che $Nx \neq 0$; Nx è un ideale di A contenuto in K e $N(Nx) = N^2x = Nx \neq 0$, quindi, per la minimalità di K in Σ, $Nx = K \ni x$. Dunque esiste $y \in N$ tale che $yx = x$. Ora, $y \in N$ è un elemento nilpotente, cioè $y^k = 0$ per qualche $k \geq 1$. Ma allora

$$x = yx = y^2x = \ldots = y^kx = 0,$$

una contraddizione. Quindi $N = \mathfrak{N}(A)^n = 0$. □

Lemma 47. *Sia A un anello, e supponiamo che A contienga un numero finito di ideali massimali $M_1, M_2, \ldots, M_n$ (non necessariamente distinti) tali che $M_1M_2 \cdots M_n = (0)$. Allora A è artiniano se e solo se è noetheriano.*

Dimostrazione. Per induzione sul numero di ideali n. Se $n = 1$, $M_1 = (0)$ e A è un campo. Sia $n \geq$ e $J = M_1 \cdots M_{n-1}$. Per ipotesi induttiva, l'anello quoziente A/J è artiniano se e solo se è noetheriano. Se $J = (0)$ abbiamo finito. Altrimenti, $J \neq 0$ e $M_nJ = 0$ e poiché M_n è un ideale massimale, vedendo J come A-sottomodulo, $M_n = Ann_A(J)$; ma allora J è un $\mathbb{K}$-modulo dove $\mathbb{K} = A/M_n$ è un campo. Quindi J è uno spazio vettoriale su $\mathbb{K}$, ed è artiniano come A-modulo se e solo se lo è come $\mathbb{K}$-spazio, ovvero se e solo se ha dimensione finita e questo avviene se e solo se è noetheriano (come $\mathbb{K}$-spazio e dunque come A-modulo). L'enunciato ora discende dalle Proposizioni 33 e 42. □

Definizione. Sia $A \neq 0$ un anello: una catena ascendente $P_0 \subset P_1 \subset \cdots \subset P_n$ di ideali distinti di A ha lunghezza n. La *dimensione* di A, $\dim(A)$, è l'estremo superiore delle lunghezze delle catene ascendenti costituite da ideali *primi* di A.

Ad esempio, dalla Proposizione 6 segue che $\dim(A) = 0$ se e solo se gli unici ideali primi di A sono gli ideali massimali. Quindi, un dominio d'integrità con domensione 0 è un campo. Ancora, un P.I.D. è un campo oppure ha dimensione 1.

Proposizione 48. *Sia A un anello Artiniano. Allora A è Noetheriano e* $\dim(A) = 0$.

Dimostrazione. ($\Rightarrow$) Sia A un anello artiniano. Allora $\dim(A) = 0$ per il punto (2) del Lemma 45. Proviamo che A è noetheriano. Per il Lemma 45, A ha un numero finito $M_1, \ldots, M_k$ di ideali massimali; sia $J = M_1 M_2 \cdots M_k$, allora $J \subseteq \mathrm{J}(A)$ e dunque, per la Proposizione 46, è nilpotente; ovvero esiste $m \geq 1$ con $J^m = (0)$. Allora

$$(0) = (M_1 M_2 \cdots M_k)^m = M_1^m \cdot M_2^m \cdots M_k^m,$$

e segue quindi dal Lemma 47 che A è noetheriano. □

Osserviamo che questo non vale per moduli: l'esempio del un gruppo abeliano U_p di prima mostra che esistono moduli Artiniani che non sono Noetheriani; ma osserviamo che, come $\mathbb{Z}$-modulo, il gruppo U_p non è finitamente generato. Si ha infatti il seguente:

Corollario 49. *Sia Aun anello e sia M un A-modulo finitamente generato. Se A è Artiniano allora è Noetheriano.*

Dimostrazione. Esercizio. □

Si può provare (come faremo con l'esercizio 40) che vale anche il viceversa della Proposizione 48, ovvero che un anello neotheriano di dimensione 0 è artiniano. Vediamo infine una proprietà degli anelli artiniani locali che spesso torna utile.

Lemma 50. *Sia A un anello artiniano locale, M il suo unico ideale massimale e $\mathbb{K} = A/M$ il campo residuo. Sono equivalenti:*

(1) *Ogni ideale di A è principale;*

(2) *M è principale;*

(3) *la dimensione di M/M^2 come $\mathbb{K}$-spazio vettoriale è al più* 1.

Dimostrazione. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) sono piuttosto ovvie. Proviamo (3) $\Rightarrow$ (1).
Se $\dim_{\mathbb{K}}(M/M^2) = 0$, allora $M = M^2$ e quindi $M = 0$ per il Lemma di Nakayama. Dunque A è un campo e tutto segue banalmente.
Sia $\dim_{\mathbb{K}}(M/M^2) = 1$. Sia $x \in M \setminus M^2$; allora $(x) + M^2 = M$, e quindi $(x) = M$ per il Corollario 27. Osserviamo anche che, per la Proposizione 46, $M = J(A)$ è nilpotente. Sia J un ideale di A che possiamo supporre diverso da (0) e da A; allora esiste un massimo intero k tale che $J \subseteq M^k = (x^k)$; ed esiste quindi $y = ax^k \in J$

(con opportuno $a \in A$) tale che $y \notin M^{k+1} = (x^{k+1})$. Di conseguenza, $a \notin M = (x)$ e dunque a è invertibile in A, quindi $x^k = a^{-1}y \in J$. Pertanto, $M^k = (x^k) \subseteq J \subseteq M^k$, e $J = M^k = (x^k)$ è un ideale principale. □

Esercizio 35. [ex 6.1 in A.M.] Sia M un A-modulo Artiniano, e $\phi : M \to M$ un omomorfismo di A-moduli. Si provi che se ϕ è iniettivo allora è un isomorfismo.

Esercizio 36. Sia $\mathbb{K}$ un campo e siano $x_1, \ldots, x_n$ indeterminate indipendenti. Si provi che $\dim(\mathbb{K}[x_1, \ldots, x_n]) \geq n$.

3.3 Decomposizione primaria di ideali

[questa sezione mette assieme alcune parti dei capitoli 4 e 7 di A.M.]

DEFINIZIONE. Un ideale Q di un anello A si dice *primario* quando $Q \neq A$ e per ogni $x, y \in A$, se $xy \in Q$ e $x \notin Q$ allora esiste $n \geq 1$ con $y^n \in Q$.

Visto al quoziente, l'ideale Q di A è primario se e solo se $A/Q \neq 0$ ed ogni divisore dello zero dell'anello quoziente A/Q è un elemento nilpotente.

Lemma 51. *Sia Q un ideale primario dell'anello A. Allora il radicale $\sqrt{Q}$ è il minimo ideale primo di A contenente Q.*

Dimostrazione. Poiché $\sqrt{Q}$ è l'intersezione degli ideali primi che contengono Q, basta provare che $\sqrt{Q}$ è primo. Siano $x, y \in A$ con $xy \in \sqrt{Q}$; allora $x^n y^n = (xy)^n \in Q$ per qualche $n \geq 1$. Se $x^n \in Q$ allora $x \in \sqrt{Q}$, altrimenti, per la primarietà di Q, esiste $m \geq 1$ tale che $y^{nm} = (y^n)^m \in Q$, dunque $y \in \sqrt{Q}$. □

ESEMPI. 1) Sia A un dominio a ideali principali; allora gli ideali primi $\neq 0$ sono gli ideali massimali. Se un ideale $I = (x) \neq (0)$ è primario, dal Lemma 51 segue che I è contenuto in un solo ideale massimale $M = (b)$; il che significa che (a meno di moltiplicazione per invertibili) b è il solo divisore irriducibile di x, quindi $x = ub^n$, con $u \in U(A)$ e $n \geq 1$, e $I = (b^n)$. Viceversa, se b è un elemento irriducibile di A e $n \geq 1$ è immediato verificare che l'ideale (b^n) è primario. In particolare, gli ideali primari di $\mathbb{Z}$ sono (0) e tutti e soli quelli del tipo (p^n) con p un primo e $n \geq 1$.

2) Sia $\mathbb{K}$ è un campo e $A = \mathbb{K}[x, y]$ l'anello dei polinomi in due indeterminate. L'ideale $I = (x, y^2)$ è primario in A: infatti $A/I \simeq \mathbb{K}[y]/(y^2)$ ed ogni divisore dello zero in questo quoziente appartiene all'ideale $(y)/(y^2)$ che è nilpotente (è il nil-radicale del quoziente). Quindi (x, y^2) è primario e $\sqrt{(x, y^2)} = (x, y)$.
L'ideale $K = (yx, y^2)$ non è primario: infatti $yx \in K$ ma $y \notin K$ e xK non è nilpotente in A/K.

3) In generale, non vale il viceversa del Lemma 51: il radicale di un ideale I può essere un ideale primo (e dunque è il minimo ideale primo contenente I) senza che I sia primario. Ad esempio, sia $n \geq 2$ e in $\mathbb{Z}[x]$ consideriamo l'ideale $I = (x^2, nx)$; per ogni $f \in (x)$ si ha $f^2 \in I$, dunque $(x) \subseteq \sqrt{I}$, d'altra parte $I \subseteq (x)$ e $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ è un dominio d'integrità, pertanto $(x) \supseteq \sqrt{I}$. Dunque $\sqrt{I} = (x)$ è un ideale primo. Ma I non è primario: $xn \in I$ mentre $x \notin I$ e $n \notin \sqrt{I}$.

Si ha tuttavia la seguente ristretta inversione del Lemma 51

Lemma 52. *Sia I un ideale proprio dell'anello A. Se $\sqrt{I}$ è un ideale massimale, I è primario. In particolare le potenze di un ideale massimale sono ideali primari.*

Dimostrazione. Sia $M = \sqrt{I}$ un ideale massimale. Allora, M è l'unico ideale massimale di A contenente I, dunque A/I è un anello locale, e di conseguenza ogni elemento in $A \setminus M$ è invertibile modulo I. Siano $x, y \in A$ con $xy \in I$. Se $y \in M = \sqrt{I}$ allora $y^n \in I$ per qualche $n \geq 1$; altrimenti esiste un inverso $b + I \in A/I$ di $y + I$, dunque $x + I = (x + I)(yb + I) = (xy)b + I = I$ e quindi $x \in I$. □

Ricordo che, se I è un ideale di un anello A e $x \in A$ allora l'insieme

$$(I : x) = \{a \in A \mid ax \in I\}$$

è un ideale A contenente I (se $x \in I$ allora $(I : x) = A$).

Lemma 53. *Sia Q un ideale primario dell'anello A, $P = \sqrt{Q}$, e sia $x \in A$. Allora*

(1) *se $x \notin Q$ allora $(Q : x)$ è primario e $\sqrt{(Q : x)} = P$;*

(2) *se $x \notin P$ allora $(Q : x) = Q$.*

Dimostrazione. (1) Se $y \in (Q : x)$ allora $xy \in Q$ e quindi, poiché Q è primario e $x \notin Q$, $y \in P$. Dunque $Q \subseteq (Q : x) \subseteq P$, quindi $P = \sqrt{Q} \subseteq \sqrt{(Q : x)} \subseteq \sqrt{P} = P$ e $\sqrt{(Q : x)} = P$. Siano ora $a, b \in A$ con $ab \in (Q : x)$ e $a \notin \sqrt{(Q : x)}$; poiché $abx \in Q$ si ha allora $bx \in Q$ da cui $b \in (Q : x)$, provando che $(Q : x)$ è primario.
(2) Segue direttamente dalla definizione di ideale primario. □

Esercizio 37. [ex 4.4 in A.M.] Si provi che nell'anello $\mathbb{Z}[x]$ l'ideale $(4, x)$ è primario ma non è la potenza di un ideale massimale.

Definizione. Sia I un ideale dell'anello A. Si dice che I è un ideale *decomponibile* se ammette una *decomposizione primaria*, cioè esiste un insieme finito $\{Q_1, \ldots, Q_n\}$ di ideali primari di A tale che

$$I = \bigcap_{i=1}^{n} Q_i. \tag{10}$$

Se, inoltre, sono soddisfatte le seguenti condizioni:

(i) i radicali $\sqrt{Q_i}$ sono tutti diversi ($i = 1, \ldots, n$), e

(ii) per ogni $1 \leq i \leq n$, si ha $\bigcap_{j \neq i} Q_j \neq I$,

allora la decomposizione in (10) si dice *irridondante*, o minimale.

Non ogni ideale I di un anello è decomponibile; ma, se lo è, allora I ammette una decomposizione primaria irridondante. Questo segue facilmente dal seguente Lemma.

Lemma 54. *Sia $n \geq 1$ e siano $Q_1, \ldots Q_n$ ideali primari di un anello A, Se $\sqrt{Q_i} = P$ per lo stesso ideale P per ogni $1 \leq i \leq n$, allora $Q = \bigcap_{i=1}^n Q_i$ è un ideale primario e $\sqrt{Q} = P$.*

Dimostrazione. $\sqrt{Q} = P$ segue dal punto (iii) della Proposizione 12. Siano $x, y \in A$ con $xy \in Q$ e $x \notin Q$; allora $x \notin Q_i$ per qualche $1 \leq i \leq n$, e poiché $xy \in Q_i$ si ha $y \in \sqrt{Q_i} = P$. Pertanto Q è primario. □

Dunque, in una decomposizione di un ideale I come in (10) possiamo rimpiazzare ideali P_i che abbiano lo stesso radicale con la loro intersezione, ottenendo una decomposizione primaria che soddisfa (i); a questo punto togliamo uno dopo l'altro gli ideali P_i che risultano superflui, fino a che sia soddisfatta anche la condizione (ii).

Vediamo una prima istanza di unicità.

Teorema 55. *Sia I un ideale decomponibile dell'anello A e sia $I = \bigcap_{i=1}^n Q_i$ una decomposizione primaria irridondante di I. Allora l'insieme $\{\sqrt{Q_i} \mid 1 \leq i \leq n\}$ coincide con l'insieme di tutti gli ideali* primi *del tipo $\sqrt{(I : x)}$ al variare di $x \in A$.*

Dimostrazione. Sia $I = \bigcap_{i=1}^n Q_i$ una decomposizione primaria irridondante dell'ideale I e, per ogni $1 \leq i \leq n$, sia $P_i = \sqrt{Q_i}$. Per ogni $x \in A$ si ha $(I : x) = \bigcap_{i=1}^n (Q_i : x)$ e dunque, per il Lemma 53

$$\sqrt{(I : x)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : x)} = \bigcap_{x \notin Q_i} P_i.$$

Se $\sqrt{(I : x)}$ è primo allora, per il Lemma 4, coincide con qualche P_i.
Viceversa, poiché la decomposizione di è irridondante, per ogni $1 \leq i \leq n$ esiste un elemento $x_i \in \left(\bigcap_{j \neq i} Q_j\right) \setminus Q_i$; dal Lemma 53 segue $\sqrt{(I : x_i)} = P_i$. □

Definizione. Sia I è un ideale decomponibile dell'anello A e $I = \bigcap_{i=1}^n Q_i$ una sua decomposizione primaria irridondante, allora il Teorema precedente dice in particolare che gli ideali primi $P_i = \sqrt{Q_i}$ ($i = 1, \ldots, n$) non dipendono dalla particolare decomposizione; tali ideali $P_1, \ldots, P_n$ si chiamano gli ideali primi *associati* a I.

Dal Teorema 55 segue che gli ideali primi associati ad I sono precisamente gli ideali del tipo $\sqrt{Ann_A(x+I)}$ (guardando A/I come A-modulo) che sono primi.
Osserviamo anche che se I è un ideale decomponibile e $P_1, \ldots, P_n$ sono gli ideali primi associati ad I, allora per la Proposizione 12,

$$P_1 \cap \ldots \cap P_n = \sqrt{Q_1 \cap \ldots \cap Q_n} = \sqrt{I}; \tag{11}$$

quindi (Lemma 4) ogni ideale primo di A contenente I contiene uno degli ideali associati $P_1, \ldots, P_n$. Un ideale Q di A è un ideale primario se e solo se $\sqrt{Q}$ è l'unico ideale primo associato a Q. D'altra parte, l'intersezione degli ideali primi associati nel membro di sinistra dell'uguaglianza (11) può anche essere ridondante, come si vede dal seguente esempio.

Esempio. Nell'anello $A = \mathbb{K}[x, y]$ ($\mathbb{K}$ un campo) si ha la decomposizione primaria

$$(xy, y^2) = (x, y)^2 \cap (y), \tag{12}$$

infatti (y) è un ideale primo di A, e (x, y) è massimale, quindi $(x, y)^2$ è primario per il Lemma 52, In questo caso, gli ideali primi associati a $I = (xy, y^2)$ sono $P_1 = (y)$ e $P_2 = (x, y)$. Gli ideali primi P_1, P_2 sono univocamente determinati, ma non lo è la decomposizione (12); ad esempio $I = (y) \cap (y^2, x)$ è una diversa decomposizione primaria di I. Si osservi che, in questo esempio $P_1 \subseteq P_2$ (si noti infatti: $P_1 = \sqrt{I}$ ma I non è primario).

Definizione. Sia I un ideale decomponibile di un anello A, gli elementi minimali rispetto all'inclusione dell'insieme degli ideali primi associati ad I si chiamano ideali primi *isolati* associati ad I (gli altri si dicono ideali primi *immersi*).
(Nell'esempio di sopra, con $I = (xy, y^2)$ nell'anello $\mathbb{K}[x, y]$, l'ideale (y) è isolato e l'ideale (x, y) immerso.)

Poiché il radicale di un ideale I è l'intersezione degli ideali primi che contengono I, dall'uguaglianza (11) e dal Lemma 4 segue subito la seguente osservazione.

Proposizione 56. *Sia I un ideale decomponibile dell'anello A. Allora ogni ideale primo contenente I contiene un ideale primo associato ad I. In particolare, l'insieme degli ideali primi isolati associati a I coincide con l'insieme degli ideali primi minimali contenenti I.*

Proposizione 57. *Sia I un ideale decomponibile dell'anello A, $I = \bigcap_{i=1}^{n} Q_i$ una sua decomposizione primaria irridondante e, per $1 \leq i \leq n$, sia $P_i = \sqrt{Q_i}$. Allora*

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

In particolare, se (0) *è decomponibile, l'insieme dei divisori dello zero di* A *è l'unione degli ideali primi associati a* 0*.*

Dimostrazione. Sia $D = \{x \in A \mid (I : x) \neq I\}$.
Se $x \in D$ esiste $y \in (I : x)$ e $y \notin I$. Allora $y \notin Q_i$ per qualche $1 \leq i \leq n$ e quindi, per il Lemma 53, $x \in (I : y) \subseteq (Q_i, y) \subseteq P_i$; dunque $x \in P_i$.
Viceversa, dal Teorema 55 segue che, per ogni $1 \leq i \leq n$, $P_i = \sqrt{(I : x)}$ per qualche $x \in D$. Dunque, se $y \in P_i$, esiste un minimo $m \geq 1$ tale che $y^m \in (I : x)$, per cui $y^{m-1}x \in (I : y)$ e $y^{m-1}x \notin I$, provando che $y \in D$. Dunque $P_i \subseteq D$ per ogni $1 \leq i \leq n$. □

Ci sposteremo tra poco al caso degli anelli Noetheriani; prima una definizione che si applica ad un ideale in un anello generico.

DEFINIZIONE. Un ideale proprio I di un anello A si dice *irriducibile* se non è intersezione di due ideali che lo contengo propriamente.
Quindi, un ideale $I \neq A$ è irriducibile se per ogni coppia di ideali J, L

$$J \cap L = I \;\Rightarrow\; I = J \text{ o } I = L.$$

Lemma 58. *In un anello Noetheriano ogni ideale proprio è intersezione di un numero finito di ideali irriducibili.*

Dimostrazione. Sia A un anello Noetheriano e supponiamo, per assurdo, che l'insieme Σ degli ideali propri di A che non sono intersezione di un numero finito di ideali irriducibili sia non vuoto. Allora, per noetherinità, Σ ha un elemento massimale H e poiché H non è irriducibile esistono ideali I, J di A con $H \subset I$, $H \subset J$, e $I \cap J = H$. Osservando che, necessariamente, I, J sono ideali propri, per la massimalità di H in Σ si ha che entrambi sono intersezione di un numero finito di ideali irriducibili. Ma allora anche H è intersezione di un numero finito di ideali irriducibili, che è una contraddizione. □

Lemma 59. *In un anello Noetheriano ogni ideale irriducibile è primario.*

Dimostrazione. Sia I un ideale irriducibile dell'anello Noetheriano A. Poiché A/I è Noetheriano, possiamo assumere $I = \{0\}$, e provare, quindi, che se (0) è irriducibile allora ogni divisore dello zero di A è nilpotente. Siano $x, y \in A$ con $xy = 0$ e $x \neq 0$; vogliamo mostrare che y è nilptente. La catena di ideali

$$Ann_A(y) \subseteq Ann_A(y^2) \subseteq \dots$$

è stazionaria: sia $n \geq 1$ con $Ann_A(y^n) = Ann_A(y^{n+1})$. Sia $u \in (x) \cap (y^n)$; esistono quindi elementi $a, b \in A$ tali che $ax = u = by^n$; ma allora $by^{n+1} = axy = 0$, quindi $b \in Ann_A(y^{n+1}) = Ann_A(y^n)$ e pertanto $u = by^n = 0$. Dunque $(x) \cap (y^n) = (0)$ e quindi, per l'irriducibilità di (0), $(y^n) = 0$ ovvero y è nilpotente. □

Dai Lemmi 58 e 59 segue immediatamente il seguente fondamentale risultato.

Teorema 60. *In un anello Noetheriano ogni ideale proprio è decomponibile.*

Esempio 1 [ex 4.5 in A.M.]. Sia $A = \mathbb{K}[x, y, z]$, dove x, y, z sono indeterminate indipendenti sul campo $\mathbb{K}$. Siano $P_1 = (x, y)$, $P_2 = (x, z)$, e $I = P_1P_2$. Allora, P_1 è il nucleo dell'omomorfismo $A \to \mathbb{K}[z]$ definito sostituendo x, y con 0; quindi, poiché $\mathbb{K}[z]$ è un dominio d'integrità, P_1 è primo; similmente P_2 è primo. Consideriamo poi $M = (x, y, z)$ che è un ideale massimale di A (è il nucleo dell'omomorfismo $A \to \mathbb{K}$ che associa ad ogni polinomio in A il suo termine noto). Osserviamo che $P_1 \cap P_2 = (x, yz) = (x) + (yz)$ e che, siccome $A = \mathbb{K} + M$, si ha $(x) = x\mathbb{K} + xM$; quindi $(x) \cap M^2 = xM = (x^2, xy, xz)$. Ora, poiché $(yz) \subseteq M$,

$$P_1 \cap P_2 \cap M^2 = ((x) + (yz)) \cap M^2 = ((x) \cap M^2) + (yz) = (x^2, xy, xz, yz) = I.$$

Questa è una decomposizione primaria di I, che si verifica facilmente essere irridondante. Gli ideali primi associati ad I sono dunque P_1, P_2, M, di cui P_1 e P_2 sono quelli isolati.

Esempio 2. Vogliamo determinare una decomposizione primaria e gli ideali primi associati all'ideale (6) dell'anello $A = \mathbb{Z}[\sqrt{-5}]$ (dove $\sqrt{-5} = i\sqrt{5}$).

Conviene interpretare $A \simeq \mathbb{Z}[x]/(x^2 + 5)$ (per cui $\sqrt{-5} = x + (x^2 + 5)$). Consideriamo la riduzione modulo 2: $\pi_2 : A \to A_2 = \mathbb{Z}_2[x]/(x^2 - 5)$; si ha $\ker(\pi_2) = (2) \supset (6)$. Inoltre in $\mathbb{Z}_2[x]$, $x^2 + 5 = x^2 + 1 = (x + 1)^2$; quindi $A_2 = \mathbb{Z}_2[x]/((x + 1)^2)$ e $(x + 1)/(x^2 + 1)$ è un ideale massimale ($x + 1$ è irriducibile in $\mathbb{Z}_2[x]$) e nilpotente di A_2; la sua immagine inversa per π_2 in A è

$$P_1 = (2, 1 + \sqrt{-5}) = \{a + b\sqrt{-5} \mid a + b \in 2\mathbb{Z}\}$$

che è un ideale massimale di A e $P_1^2 \subseteq (2)$. Dunque $P_1 = \sqrt{(2)}$ e, per il Lemma 52, (2) è un ideale primario di A.

Passiamo alla riduzione modulo 3: $\pi_3 : A \to A_3 = \mathbb{Z}_3[x]/(x^2 + 5)$, tenendo conto che $\ker(\pi_3) = (3) \supset (6)$. Ora, in $\mathbb{Z}_3[x]$, $x^2 + 5 = x^2 - 1 = (x - 1)(x + 1)$; dunque A_3 ha due ideali primi, che sono quelli massimali, $(x - 1)/(x^2 - 1)$ e $(x + 1)/(x^2 - 1)$, le cui immagini inverse per π_3 in A sono, rispettivamente,

$$P_2 = (3, 1 - \sqrt{-5}) = \{a + b\sqrt{-5} \mid a + b \in 3\mathbb{Z}\},$$

$$P_3 = (3, 1 + \sqrt{-5}) = \{a + b\sqrt{-5} \mid a - b \in 3\mathbb{Z}\},$$

che sono ideali massimali (dunque primari) di A. Infine si ha, con semplici calcoli,

$$(2) \cap P_2 = \{a + b\sqrt{-5} \mid a + b \in 6\mathbb{Z}\},$$

$(2) \cap P_3 = \{a + b\sqrt{-5} \mid a - b \in 6\mathbb{Z}\}$,

$P_2 \cap P_3 = (3)$, e infine

$$(2) \cap P_2 \cap P_3 = (6),$$

che è quindi una decomposizione primaria irridondante dell'ideale (6) nell'anello A. Di conseguenza, gli ideali primi associati sono P_1, P_2, P_3, e sono tutti isolati.

Esercizio 38. [ex 4.7 in A.M.] Sia A un anello e $A[x]$ l'anello dei polinomi a coefficienti in A. Se I è un ideale di A, si denota con $I[x]$ è l'insieme degli elementi di $A[x]$ i cui coefficienti appartengono ad I. Sia I un ideale di A: si dimostrino i seguenti fatti.

(i) I è un ideale primo di A se e solo se $I[x]$ è un ideale primo di $A[x]$.

(ii) $\sqrt{I[x]} = \sqrt{I}[x]$; inoltre I è primario in A se e solo se $I[x]$ è primario in $A[x]$.

(iii) Se $I = \bigcap_{i=1}^{n} Q_i$ è una decomposizione primaria irridondante dell'ideale I, allora $I[x] = \bigcap_{i=1}^{n} Q_i[x]$ è una decomposizione primaria irridondante di $I[x]$ in $A[x]$.

(iv) Se P è un ideale primo isolato associato all'ideale decomponibile I di A, allora $P[x]$ è un ideale primo isolato associato a $I[x]$ in $A[x]$.

Esercizio 39. [ex 7.19 in A.M.] Sia I ideale dell'anello noetheriano A e siano

$$\bigcap_{i=1}^{n} R_i = I = \bigcap_{i=1}^{m} J_i$$

due decomposizioni minimali di I come intersezione di ideali irriducibili di A. Si provi che $n = m$ e che esiste una permutazione π di $\{1, \ldots, n\}$ tale che $\sqrt{R_i} = \sqrt{J_{\pi(i)}}$ per ogni $i \in \{1, \ldots, n\}$.

Esercizio 40. Si provi che un anello noetheriano A con $\dim(A) = 0$ è artiniano (per il viceversa vedi la Proposizione 48).

Esercizio 41. [ex 8.7 in A.M.] Sia Q un ideale primario dell'anello noetheriano A, e sia $P = \sqrt{Q}$; sia quindi $\mathcal{L}$ l'insieme di tutti gli ideali primari R di A tali che $Q \subseteq R \subseteq P$. Si provi che tutte le catene in $(\mathcal{L}, \subseteq)$ sono finite e di lunghezza limitata; si provi che le catene massimali hanno la stessa lunghezza.

Esercizio 42. [ex 8.2 in A.M.] Sia A un anello Noetheriano. Si provi che le seguenti proprietà sono equivalenti.

(1) A è Artiniano;

(2) $Spec(A)$ è discreto e finito;

(3) $Spec(A)$ è discreto.

Soluzioni di alcuni esercizi.

Esercizio 31 – Soluzione. Sia $\phi : M \to M$ suriettivo. Per ogni $j \geq 1$ sia $N_j = \ker(\phi^j)$; poichè, per $j \leq k$, $\ker(\phi^j) \subseteq \ker(\phi^k)$, tali ideali costituiscono una catena ascendente e pertanto esiste $n \geq 1$ tale che $N_n = N_{n+1}$. Sia $b \in \ker(\phi)$; poiché ϕ è suriettiva, anche ϕ^n è suriettiva, dunque esiste $a \in M$ tale che $b = \phi^n(a)$. Ma allora $\phi^{n+1}(a) = \phi(b) = 0$; quindi $a \in \ker(\phi^{n+1}) = \ker(\phi^n)$ e $b = \phi^n(a) = 0$. Quindi $\ker(\phi) = \{0\}$ e ϕ è un isomorfismo. ∎

Esercizio 32 – Soluzione. M è un A-modulo finitamente generato; siano $x_1, \ldots, x_n \in M$ tali che $M = Ax_1 + \cdots + Ax_n$. Per ogni $1 \leq i \leq n$ sia $\phi_i : A \to Ax_i$ definita da $\phi_i(a) = ax_i$, per ogni $a \in A$: Ax_i è un A-modulo, ϕ_i un omomorfismo suriettivo di A-moduli, e

$$K_i = \ker(\phi_i) = Ann_A(Ax_i) = \{a \in A \mid ax_i = 0\}.$$

Per il Teorema di omomorfismo si ha quindi $A/K_i \simeq Ax_i$, in particolare $A_i = A/K_i$ è Noetheriano (come A-modulo e come anello). Ora, ponendo, per ogni $a \in A$, $\pi(a) = (a + K_1, \ldots, a + K_n)$, si definisce una applicazione $\pi : A \to A_1 \oplus \cdots \oplus A_n$ che è un omomorfismo di A-moduli, ed inoltre

$$\ker(\pi) = \bigcap_{i=1}^{n} K_n = \bigcap_{i=1}^{n} Ann_A(Ax_i) = Ann_A(M) = \mathfrak{I}.$$

Dunque $A/\mathfrak{I}$ è un A-modulo isomorfo a $\mathrm{Im}(\pi)$, che è un sottomodulo di $A_1 \oplus \cdots \oplus A_n$. Poiché $A_1 \oplus \cdots \oplus A_n$ è Noetheriano per la Proposizione 33, $A/\mathfrak{I}$ è Noetheriano come A-modulo, e dunque come anello. ∎

Esercizio 33 – Soluzione. Poiché A non è Noetheriano, Σ non è vuoto (Corollario 37) e, dato che A è generato da 1, ogni elemento di Σ è un ideale proprio. Sia $(J_\lambda)_{\lambda \in \Lambda}$ una catena in Σ (ordinato per inclusione), e $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. Poiché J non è finitamento generato, $J \in \Sigma$. Dunque a Σ si può applicare il Lemma di Zorn, che assicura l'esistenza di elementi massimali.
Sia ora P un elemento massimale in Σ. Per quanto osservato, $P \neq A$. Siano $x, y \in A$ tali che $xy \in A$ e supponiamo $x \notin P$. Allora l'ideale $P + (x)$ non appartiene a Σ, dunque è finitamente generato. Siano $b_1, \ldots, b_n \in P$, $a_1, \ldots, a_n \in A$ tali che

$$P + (x) = (b_1 + a_1 x, \ldots, b_n + a_n x). \tag{13}$$

Consideriamo l'ideale $D = (P : (x)) = \{a \in A \mid ax \in P\}$, osservando che $y \in D \supseteq P$. Sia, per assurdo, $y \notin P$, allora $D \notin \Sigma$, dunque D è finitamente generato, e di conseguenza anche Dx (che è un ideale di A) è finitamente generato. Sia $b \in P$; da (13)

segue che esistono $x_1, \cdots, x_n \in A$ e $u \in A$ tale che

$$b = x_1 b_1 + \cdots + x_n b_n + ux$$

Ora, siccome $ux = b - (x_1 b_1 + \cdots x_n b_n) \in P$, si ha che u appartiene a D. Dunque $b \in (b_1, \ldots, b_n) + Dx$. Poiché $Dx \subseteq P$, si conclude che $P = (b_1, \ldots, b_n) + Dx$, da cui la contraddizione che P è finitamente generato. ∎

Esercizio 35 – Soluzione. Per ogni $n \geq 1$ si ha $\mathrm{Im}(\phi^n) \supseteq \mathrm{Im}(\phi^{n+1})$, quindi $\mathrm{Im}(\phi) \supseteq \mathrm{Im}(\phi^2) \supseteq \ldots$ è una catena discendente di sottomoduli di M; poiché M è artiniano esiste $n \geq 1$ tale che $\mathrm{Im}(\phi^n) = \mathrm{Im}(\phi^{n+1})$. Per ogni $y \in M$, esiste pertanto $x \in M$ tale che $\phi^n(y) = \phi^n(\phi(x))$ e dunque, poiché ϕ^n, come ϕ, è iniettiva, $y = \phi(x) \in \mathrm{Im}(\phi)$. Quindi ϕ è suriettiva e pertanto un isomorfismo. ∎

Esercizio 38 – Soluzione. Sia I un ideale di A; il punto di partenza è l'osservare che $I[x]$ è il nucleo dell'omomorfismo di riduzione modulo I, $A[x] \to (A/I)[x]$, e quindi che $A[x]/I[x] \simeq (A/I)[x]$.

(i) $I[x]$ è un ideale primo di $A[x]$ se e solo se $0 \neq A[x]/I[x] \simeq (A/I)[x]$ è un dominio d'integrità, e ciò avviene se e solo se A/I è un dominio d'integrità, ovvero se e solo se I è un ideale primo di A.

(ii) Per la Proposizione 13(i) si ha $\mathfrak{N}((A/I)[x]) = \mathfrak{N}(A/I)[x] = (\sqrt{I}/I)[x]$; dunque se ϕ è l'isomorfismo $(A/I)[x] \to A[x]/I[x]$ indotto dalla riduzione modulo I,

$$\sqrt{I[x]}/I[x] = \mathfrak{N}(A[x]/I[x]) = \phi(\sqrt{I}/I[x]) = \sqrt{I}[x]/I[x],$$

e quindi $\sqrt{I[x]} = \sqrt{I}[x]$.

Per la seconda affermazione ricordiamo che I è primario se e solo se $I \neq A$ ed ogni divisore dello zero di A/I appartiene a $\sqrt{I}/I$. Applicando ancora l'isomorfismo $A[x]/I[x] \simeq (A/I)[x]$ e l'esercizio 8, si ha che, per $f \in A[x]$, $f + I[x]$ è un divisore dello zero in $A[x]/I][x]$ se e solo se $f \notin I[x]$ ed esiste $a \in A \setminus I$ tale che $af \in I[x]$; dunque tutti i coefficienti di f che non appartengono a I sono divisori dello zero di A/I. Quindi, se I è primario in A, tutti i coefficienti di f sono nilpotenti modulo I, ovvero $f \in \sqrt{I}[x]$, e pertanto, per quanto provato sopra, $f + I[x]$ è nilpotente in $A[x]/I[x]$, provando che $I[x]$ è un ideale primario di $A[x]$. Viceversa, sia $I[x]$ primario in $A[x]$ e $a + I$ un un divisore dello zero di A/I, allora $a + I[x]$ è un divisore dello zero di $A[x]/I[x]$, dunque $a \in \sqrt{I[x]} = \sqrt{I}[x]$ e quindi $a \in \sqrt{I}$.

I punti (iii) e (iv) seguono facilmente dai due precedenti e dall'isomorfismo $A[x]/I[x] \simeq (A/I)[x]$. ∎

Esercizio 40 – Soluzione. Osserviamo che in un anello di dimensione 0 ogni ideale primo è massimale. Sia quindi A un anello neotheriano di dimensione 0. Allora l'ideale

(0) è decomponibile; siano $P_1, \ldots, P_n$ gli ideali primi associati a (0) che, per quanto osservato, sono ideali massimali. Allora

$$\mathfrak{N}(A) = \sqrt{(0)} = P_1, \cap \cdots \cap P_n \supseteq P_1 \cdots P_n.$$

Ora, poiché A è noetheriano, $\mathfrak{N}(A)$ è un ideale nilpotente per la Proposizione 40, dunque esiste $m \geq 1$ tale che $(P_1 \cdots P_n)^m = \mathfrak{N}(A)^m = 0$. Si conclude che A è artiniano per il Lemma 47. ∎

Esercizio 42 – Soluzione. (1) $\Rightarrow$ (2). Sia A un anello artiniano; allora, per per il Lemma 45, $Spec(A)$ è finito. Sia $Spec(A) = \{P_1, \ldots, P_n\}$; per ogni $1 \leq i \leq n$ dal Lemma 4 segue che esiste $a \in \cap_{j \neq i} P_j$ e $a \notin P_i$. Allora, per definizione $\mathsf{X}_a = \{P_i\}$ è un aperto in $Spec(A)$, che dunque risulta uno spazio discreto.

(2) $\Rightarrow$ (3) è ovvio.

(3) $\Rightarrow$ (1). Sia $Spec(A)$ uno spazio discreto e proviamo che $\dim(A) = 0$. Poiché A è noetheriano per ipotesi, la conclusione segue per l'esercizo 40. Supponiamo P, Q siano due ideali primi di A (quindi punti in $Spec(A)$), con $Q \subseteq P$. Allora, per ogni elemento X_f della base di aperti nella topologia di Zariski, se $P \in \mathsf{X}_f$ allora $f \notin P$, dunque $f \notin Q$ e $Q \in \mathsf{X}_f$. Siccome $Spec(A)$ è discreto si conclude che Q coincide con P, provando che la dimensione di A è 0. ∎

4 Frazioni e localizzazione

[questa parte è un estratto del capitolo 3 di A.M.]

4.1 Frazioni.

La procedura vista nel corso di Algebra 1 per immergere un dominio d'integrità nel suo campo delle frazioni si può generalizzare in modo da poter essere applicata anche ad anelli A che non siano domini d'integrità, a condizione di esercitare una selezione preliminare dell'insieme degli elementi dell'anello A che si vuole 'far diventare invertibili'.

DEFINIZIONE. Sia A un anello. Un sottoinsieme S di A si dice *moltiplicativamente chiuso* se $0 \notin S$, $1 \in S$ e $xy \in S$ per ogni $x, y \in S$. In altri termini, un sottoinsieme moltiplicativamente chiuso[1] di A è un sottomonoide del monoide moltiplicativo $A \setminus \{0\}$.

ESEMPI. 1) Se a è un elemento non nilpotente di A, allora $\{a^n \mid n \geq 0\}$ è moltiplicativamente chiuso.
2) Se I è un ideale proprio di A allora $1 + I = \{1 + x \mid x \in I\}$ è un insieme moltiplicativamente chiuso.
3) Insiemi moltiplicativamente chiusi interessanti sono i complementari di un ideale primo: se P è un ideale primo dell'anello A allora $S = A \setminus P$ è, per definizione, moltiplicativamente chiuso (in questa tipologia rientra il caso in cui A è un dominio d'integrità e $P = (0)$).

Sia S un sottoinsieme moltiplicativamente chiuso di A: sull'insieme $A \times S$ si definisce un relazione $\sim$ ponendo, per ogni $(a, x), (b, y) \in A \times S$,

$$(a, x) \sim (b, y) \;\Leftrightarrow\; (ay - bx)u = 0 \text{ per qualche } u \in S.$$

Si verifica agevolmente che $\sim$ è una relazione d'equivalenza su $A \times S$. Si denota con $S^{-1}A$ l'insieme quoziente $(A \times S)/\!\sim$ e, per ogni $(a, s) \in A \times S$, con a/s la sua classe di equivalenza; quindi

$$S^{-1}A = \{a/s \mid (a, s) \in A \times S\}.$$

Sull'insieme $S^{-1}A$ si definiscono operazioni di somma e prodotto nel modo naturale; per ogni $a/s, b/t \in S^{-1}A$;

$$\begin{aligned} a/s + b/t &= (at + bs)/st \\ a/s \cdot b/t &= ab/st. \end{aligned} \tag{14}$$

Avendo controllato che tali definizioni sono ben poste (esercizio), si verifica senza difficoltà che, con tali operazioni, $S^{-1}A$ è un anello non banale, con identità $1_{S^{-1}A}$ la

[1] Normalmente, nella definizione di insieme moltiplicativamente chiuso si ammette anche il caso in cui $0 \in S$; ma questo eventualità, in quel che segue, porta alla costruzione dell'anello banale e quindi ha poca rilevanza, per cui preferiamo escludere questo caso per definizione.

classe $1/1$. Lo zero è la classe $0/1$ e per ogni $s,t \in S$ si ha $s/t \cdot t/s = 1/1 = 1$, quindi s/t è invertibile in $S^{-1}A$. Inoltre, c'è un omomorfismo naturale $f : A \to S^{-1}A$, dato da $f(a) = a/1$ per ogni $a \in A$ (per quanto osservato $f(S) \subseteq U(S^{-1}A)$; questo omomorfismo può non essere iniettivo (si veda, più avanti, l'esempio 4.): infatti $\ker(f) = \{a \in A \mid \exists s \in S : as = 0\}$.
Questo anello $S^{-1}A$ si chiama *anello delle frazioni* di A rispetto a S. Si riconoscerà senz'altro che se D è un dominio d'integrità e $S = D \setminus \{0\}$ allora $S^{-1}A$ è il *campo delle frazioni* di D. Come nel caso del campo delle frazioni, anche gli anelli di frazioni soddisfano una proprietà universale (si può dire di minimalità).

Proposizione 61. *Sia S un sottoinsieme moltiplicativamente chiuso dell'anello A e sia $\phi : A \to B$ un omomorfismo di anelli tale che $\phi(S) \subseteq U(B)$. Allora esiste, ed è unico, un omomorfismo $\bar{\phi} : S^{-1}A \to B$ tale che $\bar{\phi}(a/1) = \phi(a)$ per ogni $a \in A$.*

Dimostrazione. (esistenza) Per ogni $a/s \in S^{-1}A$ si pone $\bar{\phi}(a/s) = \phi(a)\phi(s)^{-1}$. Questo è ben definito: infatti se $a/s = b/t$ allora $(at - bs)u = 0$ per qualche $u \in S$, quindi, poiché $\phi(u)$ è invertibile in B,

$$0 = \phi(0) = \phi(at - bs)\phi(u) = \phi(at - bs) = \phi(a)\phi(t) - \phi(b)\phi(s),$$

da cui $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$. Verificata la buona definizione, è immediato vedere che $\bar{\phi}$ è un omomorfismo, e che per ogni $a \in A$, $\bar{\phi}(a/1) = \phi(a)\phi(1)^{-1} = \phi(a)$.
(unicità) Sia $\psi : S^{-1}A \to B$ un omomorfismo tale che $\psi(a/1) = \phi(a)$ per ogni $a \in A$. Allora, per ogni $a/s \in S^{-1}A$,

$$\psi(a/s) = \psi(a/1 \cdot (s/1)^{-1}) = \psi(a/1)\psi(s/1)^{-1} = \phi(a)\phi(s)^{-1} = \bar{\phi}(a/s);$$

dunque $\psi = \bar{\phi}$. □

Esempi. 1. Come già osservato, se D è un dominio d'integrità, allora $D^* = D \setminus \{0\}$ è moltiplicativo e $(D^*)^{-1}D$ è il campo delle frazioni di D.
2. In $A = \mathbb{Z}$ sia p un primo e $S = \{p^n \mid n \in \mathbb{N}\}$. Allora

$$S^{-1}\mathbb{Z} = \mathbb{Z}[1/p] = \left\{ \frac{m}{p^n} \in \mathbb{Q} \;\middle|\; m \in \mathbb{Z},\, n \in \mathbb{N} \right\}$$

(questa identità e quelle degli esempi seguenti si intendono a meno di isomorfismo e possono essere facilmente dimostrate utilizzando la Proposizione 61).
3. In $A = \mathbb{Z}$ sia p un primo e $S = \mathbb{Z} \setminus p\mathbb{Z}$. Allora

$$S^{-1}\mathbb{Z} = \mathbb{Z}_{p\mathbb{Z}} = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; p \not| n \right\}.$$

4. Sia $A = \mathbb{Z}/12\mathbb{Z}$ e $S = \{\bar{1}, \bar{3}, \bar{9}\}$ (dove, per $z \in \mathbb{Z}$, $\bar{z} = z + 12\mathbb{Z}$). Ponendo, per ogni $\bar{a} \in A$, $\phi(\bar{a}) = a + 4\mathbb{Z}$ si definisce un omomorfismo $A \to \mathbb{Z}/4\mathbb{Z}$. Osserviamo che $\phi(S) = \{1 + 4\mathbb{Z}, -1 + 4\mathbb{Z}\} = U(\mathbb{Z}/4\mathbb{Z})$, quindi, per la Proposizione 61, esiste un omomorfismo $\bar{\phi} : S^{-1}A \to \mathbb{Z}/4\mathbb{Z}$, e siccome ϕ è suriettivo anche $\bar{\phi}$ lo è. Se $\bar{a}/\bar{s} \in \ker(\bar{\phi})$ allora $\phi(\bar{a}) = 0$, dunque $a \in 4\mathbb{Z}$ e allora, nell'anello A

$$(\bar{a} - \bar{0})\bar{3} = \bar{0}$$

che significa, in $S^{-1}A$, $\bar{a}/1 = 0$ e dunque $\bar{a}/\bar{s} = 0$. Quindi $\bar{\phi}$ è un isomorfismo.

Vediamo ora come, fissato un sottoinsieme moltiplicativamente chiuso S di un anello A, la procedura frazionaria si comporta rispetto agli ideali. Se I è un ideale di A, scriviamo

$$S^{-1}I = \{a/s \in S^{-1}A \mid a \in I, s \in S\}.$$

Nei prossimi lemmi si assume l'ipotesi comune che S sia un sottoinsieme moltiplicativamente chiuso dell'anello A, e con f si denota l'omomorfismo $f : A \to S^{-1}A$ definito da $f(a) = a/1$ per ogni $a \in A$.

Lemma 62. *Sia I un ideale di A, allora $S^{-1}I$ è un ideale di $S^{-1}A$, ed è proprio se e solo se $I \cap S = \emptyset$.*

Dimostrazione. Siano $a, a' \in I$ e $s, s' \in S$; allora, poiché I è un ideale e S è moltiplicativamente chiuso, $a/s - a'/s' = (as' - a's)/ss' \in S^{-1}I$; inoltre, se $b/t \in S^{-1}A$, $(b/t)(a/s) = ba/st \in S^{-1}I$. Quindi $S^{-1}I$ è un ideale di $S^{-1}A$.
Ora, $S^{-1}I = S^{-1}A$ se e solo se esistono $a \in I$ e $s \in S$ tali che $a/s = 1/1$, ovvero esiste $t \in S$ con $0 = (a - s)t = at - st$, quindi $as = st \in I \cap S$. Dunque $S^{-1}I = S^{-1}A$ se e solo se $I \cap S \neq \emptyset$. □

Lemma 63. *Siano I, J ideali di A.*

(1) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;

(2) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;

(3) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$;

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

Dimostrazione. (1) L'inclusione $S^{-1}(I + J) \subseteq S^{-1}I + S^{-1}J$ è ovvia. Viceversa, siano $a \in I, b \in J$, $s, t \in S$; allora $a/s + b/t = (at + bs)/st \in S^{-1}(I + J)$, così provando l'inclusione inversa.

(2) Anche qui, l'inclusione $(S^{-1}I)(S^{-1}J) \subseteq S^{-1}(IJ)$ è immediata. Viceversa, il generico generatore di $S^{-1}(IJ)$ è del tipo ab/s con $a \in I, b \in J, s \in S$; si ha però $ab/s = (s/1)(a/s)(b/s) \in (S^{-1}I)(S^{-1}J)$, il che implica l'inclusione inversa.

(3) Ancora, l'inclusione $S^{-1}(I \cap J) \subseteq S^{-1}I \cap S^{-1}J$ è ovvia. Viceversa, se $a \in I, b \in J$ e $s, t \in S$ sono tali che $a/s = b/t \in S^{-1}I \cap S^{-1}J$ allora $(at - bs)u$ per qualche $u \in S$, quindi $c = atu = bsu \in I \cap J$ e dunque $a/s = c/tus \in S^{-1}(I \cap J)$ ed anche l'inclusione inversa è provata.

(4) Sia $x \in \sqrt{I}$ con $x^n \in I$ per un $n \geq 1$, allora $(x/s)^n = x^n/s^n \in S^{-1}I$; quindi $S^{-1}\sqrt{I} \subseteq \sqrt{S^{-1}I}$. Viceversa, siano $a/s \in S^{-1}A$ e $n \geq 1$ tali che $(a/s)^n \in S^{-1}I$; allora $a^n/s^n = b/1$ per qualche $b \in I$, ovvero esiste $u \in S$ con $(a^n - bs^n)u = 0$, quindi $(a^n - bs^n)u^n = 0$, pertanto $(au)^n = bs^n u^n \in I$ e $a/s = (au)/su \in S^{-1}\sqrt{I}$. □

Denotiamo ora con $\mathcal{I}_S(A)$ l'insieme di tutti gli ideali I di A tali che $I \cap S = \emptyset$ e con $\mathcal{L} = \mathcal{L}(S^{-1}A)$ l'insieme degli ideali propri di $S^{-1}A$. Dal Lemma 62 segue che porre $I \mapsto S^{-1}I$ definisce una applicazione Δ da $\mathcal{I}_S(A)$ in $\mathcal{L}$. Nell'altro verso, poiché $f : A \to S^{-1}A$ è un omomorfismo, sappiamo che, per ogni $L \in \mathcal{L}$, l'immagine inversa $f^{-1}(L)$ è un ideale di A. Chiaramente, $f^{-1}(S^{-1}I) \supseteq I$, quindi per il Lemma 62, $L \mapsto f^{-1}(L)$ definisce un'applicazione Θ da $\mathcal{L}$ in $\mathcal{I}_S(A)$. Il prossimo Lemma mostra in particolare che $\Delta \circ \Theta$ è l'identità su $\mathcal{L}$.

Lemma 64. (i) *Sia L un ideale di $S^{-1}A$. Allora $L = S^{-1}(f^{-1}(L))$.*

(ii) *Sia P ideale primo di A con $P \cap S = \emptyset$, allora $f^{-1}(S^{-1}P) = P$.*

Dimostrazione. (i) Per la teoria generale degli omomorfismi di anelli

$$I = f^{-1}(L) = \{a \in A \mid a/1 \in L\}$$

è un ideale di A. Se $a \in I$ e $s \in S$, allora $a/s = (1/s)(a/1) \in L$; dunque $S^{-1}I \subseteq L$. Viceversa, sia $b/s \in L$, allora $b/1 = (s/1)(b/s) \in L$, dunque $b \in I$ e $b/s \in S^{-1}I$, provando l'inclusione $L \subseteq S^{-1}I$.

(ii) Sia P ideale primo di A on $P \cap S = \emptyset$. Chiaramente, $P \subseteq f^{-1}(S^{-1}P)$. Viceversa, sia $b \in f^{-1}(S^{-1}P)$; allora esistono $a \in P$, $s, u \in S$ tali che $(bs - a)u = 0$, cioè $bsu = au \in P$. Poiché P è primo e $su \in S \subseteq A \setminus P$, si ha $b \in P$, provando l'inclusione $f^{-1}(S^{-1}P) \subseteq P$. □

C'è quindi una qualche corrispondenza tra gli ideali di A (che sono disgiunti da S) e gli ideali di $S^{-1}A$; come suggerisce il Lemma 64, questo è molto stretta per ideali primi.

Proposizione 65. *Siano $\mathcal{P}_S$ l'insieme degli ideali primi P di A tali che $P \cap S = \emptyset$, e $\mathcal{I}$ quello degli ideali primi di $S^{-1}A$. Allora l'applicazione definita da $P \to S^{-1}P$ (per ogni $P \in \mathcal{P}_S$) è una biezione $\mathcal{P}_S \to \mathcal{I}$.*

Dimostrazione. In virtù del Lemma 64, è sufficiente provare che se $P \in \mathcal{P}_S$ allora $S^{-1}P$ è un ideale primo di $S^{-1}A$, e che se $L \in \mathcal{I}$ allora $f^{-1}(L)$ è un ideale primo di A. La seconda condizione è un fatto generale per omomorfismi di anelli.

Sia allora $P \in \mathcal{P}_S$. Per il Lemma 62, $S^{-1}P$ è un ideale proprio di $S^{-1}A$. Siano $a, b \in A$, $s, t \in S$ con $(a/s)(b/t) \in S^{-1}P$; allora, poiché $S^{-1}P$ è un ideale, $ab/1 \in S^{-1}P$; dunque esistono $x \in P$, $u, w \in S$ tali che $(abu - x)w = 0$, quindi $abuw = xw \in P$. Siccome P è primo e disgiunto da S, deve essere $ab \in P$ e ancora $a \in P$ oppure $b \in P$; ovvero uno tra a/s e b/t appartiene a $S^{-1}P$, che quindi è provato essere primo. □

Corollario 66. *Sia S un sottoinsieme moltiplicativamente chiuso dell'anello A. Allora $\mathfrak{N}(S^{-1}A) = S^{-1}(\mathfrak{N}(A)))$.*

Dimostrazione. Tenendo conto che se I è un ideale di A con $I \cap S \neq \emptyset$, allora $S^{-1}I = S^{-1}A$, dalla Proposizione 65, e con le notazioni della stessa, si deduce

$$\mathfrak{N}(S^{-1}A) = \bigcap_{P \in \mathcal{P}_S} S^{-1}P = \bigcap_{P \text{ primo}} S^{-1}P \supseteq S^{-1}(\mathfrak{N}(A)).$$

Viceversa, sia a/s un elemento nilpotente di $S^{-1}A$ (con $a \in A$ e $s \in S$), e $n \geq 0$ tale che $0/1 = (a/s)^n = a^n/s^n$; allora esiste $u \in S$ tale che $a^n u = 0$. Dunque $0 = (au)^n$ e $a/s = au/su \in S^{-1}(\mathfrak{N}A)$. Quindi, $\mathfrak{N}(S^{-1}A) \subseteq S^{-1}(\mathfrak{N}(A))$ e la dimostrazione è completa. □

Corollario 67. *Sia S un sottoinsieme moltiplicativamente chiuso dell'anello A. Se A è noetheriano allora $S^{-1}A$ è noetheriano.*

Dimostrazione. Viene subito dal Lemma 64. Infatti, se Σ è un insieme di ideali propri di $S^{-1}A$, allora $\Sigma = \{S^{-1}(I) | I \in \Delta\}$, dove $\Delta = \{f^{-1}(L) \mid L \in \Sigma\}$ è un insieme di ideali di A disgiunti da S. Per noetherianità, Δ ha un elemento massimale J, e per il punto (i) del Lemma 64, $S^{-1}J$ è un elemento massimale di Σ. Ciò prova che $S^{-1}A$ è noetheriano. □

NOTA. Una dimostrazione del tutto analoga mostra che il Corollario vale sostituendo "noetheriano" con "artiniano".

Qualcosa di simile a quanto visto nel Lemma 64 per ideali primi vale per ideali primari.

Lemma 68. *Siano S un sottoinsieme moltiplicativamente chiuso dell'anello A, Q un ideale primario di A e $P = \sqrt{Q}$.*

(1) *Se $S \cap P \neq \emptyset$, allora $S^{-1}Q = S^{-1}A$.*

(2) *Se $S \cap P = \emptyset$, allora $S^{-1}Q$ è primario in $S^{-1}A$ e $\sqrt{S^{-1}Q} = S^{-1}P$.*

Dimostrazione. Esercizio. □

A partire da ciò si controlla facilmente il frazionamento di ideali decomponibili.

Proposizione 69. *Siano S un sottoinsieme moltiplicativamente chiuso dell'anello A, I un ideale decomponibile di A, $I = \bigcap_{i=1}^{n} Q_i$ una decomposizione primaria irridondante di I e, pr ogni $1 \leq i \leq n$, $P_i = \sqrt{Q_i}$. Inoltre, gli indici siano assegnati in modo che $P_i \cap S = \emptyset \Leftrightarrow 1 \leq i \leq m$ (con $m \leq n$). Allora*

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i,$$

è una decomposizione primaria irridondante dell'ideale $S^{-1}I$.

Esercizio 43. Sia S un sottoinsieme moltiplicativamente chiuso dell'anello A; si provi che $S^{-1}A$ è isomorfo ad A se e soltanto se $S \subseteq U(A)$.

Esercizio 44. [Coroll. 3.2 in A.M.] Sia $\alpha : A \to B$ un omomorfismo di anelli, e sia S un sottoinsieme moltiplicativamente chiuso di A tale che

(i) $\alpha(S) \subseteq U(B)$,

(ii) per ogni $a \in A$, $\alpha(a) = 0 \Rightarrow as = 0$ per qualche $s \in S$

(iii) $B = \{\alpha(a)\alpha(s)^{-1} \mid a \in A.s \in S\}$.

Si provi che B è isomorfo a $S^{-1}A$.

Esercizio 45. [ex 3.2 in A.M.] Sa I un ideale proprio dell'anello A e $S = 1 + I$. Si provi che $S^{-1}I \subseteq \mathrm{J}(S^{-1}A)$.

Esercizio 46. [ex 3.7 in A.M.] Un sottoinsieme moltiplicativamente chiuso S di un anello A si dice *saturo* se per ogni $x, y \in A$,

(1) Si provi che S è saturo se e solo se $A \setminus S$ è unione di ideali primi. Si dimostri quindi che per ogni sottoinsieme moltiplicativamente chiuso S di A esiste un minimo sottoinsieme saturo $\overline{S}$ (detto *saturazione* di S) tale che $S \subseteq \overline{S}$.

(2) Si determini $\overline{S}$ nel caso $S = 1 + I$ dove I è un ideale proprio di A.

4.2 Localizzazione.

DEFINIZIONE. Sia P un ideale primo dell'anello A e $S = A \setminus P$. L'anello di frazioni $S^{-1}A$ si dice *localizzazione di A a P* e si denota con A_P.

Ad esempio, se D è un dominio d'integrità, l'ideale nullo (0) è primo e la localizzazione $A_{(0)}$ è il campo delle frazioni di D. Nel caso $A = \mathbb{Z}$ le altre possibili localizzazioni di $\mathbb{Z}$ sono descritte nell'esempio 3 di sopra.

Vediamo la ragione del termine: sia P un ideale primo dell'anello A e A_P la localizzazione a P, allora

$$M = S^{-1}P = \{a/s \in A_P \mid a \in P, s \in A \setminus P\}$$

è un ideale di A_P (Lemma 62). Inoltre, se $t/s \in A_P \setminus M$ allora $t \in A \setminus P$ e dunque t/s è invertibile in A_P. Quindi A_P è un *anello locale* ed M il suo unico ideale massimale. L'applicazione $\hat{f} : A/P \to A_P/M$ definita da $\hat{f}(a+P) = a/1 + M$, per ogni $a \in A$ (è una buona definizione) è un omomorfismo iniettivo; infatti $a + P \in \ker(\hat{f})$ se e solo se $a/1 \in M$, ovvero esiste $y \in A \setminus P$ tale che $ay \in P$, cha si verifica se e solo se $a \in P$ (P è primo); inoltre, per ogni $a \in A,\ s \in A \setminus P$,

$$a/s + M = (a+M)(s+M)^{-1} = \hat{f}(a+P)\hat{f}(s+P)^{-1}.$$

Si deduce quindi la seguente osservazione.

Proposizione 70. *Sia P un ideale primo dell'anello A; allora il campo residuo A_P/M è (isomorfo a) il campo delle frazioni del dominio A/P.*

Come caso particolare della Proposizione 65, si ha:

Proposizione 71. *Sia P un ideale primo dell'anello A; allora l'insieme degli ideali primi di A_P è in corrispondenza biunivoca con l'insieme degli ideali primi di A che sono contenuti in P.*

Dal Corollario 67 segue poi immediatamente:

Proposizione 72. *Sia P un ideale primo dell'anello noetheriano A; allora A_P è noetheriano.*

Esempio 1. Sia f è un polinomio irriducible dell'anello $A = \mathbb{K}[x]$, con $\mathbb{K}$ campo; allora l'ideale $P = (f)$ è primo (di fatto, è massimale) e, posto $S = A \setminus P$, $A_P = S^{-1}A$ è contenuto nel campo delle frazioni $\mathbb{K}(x)$; precisamente,

$$A_P = \{h/g \mid h, g \in A,\ g \notin P\} = \{h/g \mid h, g \in A, (f,g) = 1\}.$$

Ora, i soli ideali primi di A contenuti in P sono P stesso e (0); quindi l'anello locale A_P ha solo due ideali primi: $S^{-1}(0) = (0)$ e $S^{-1}P$ (cioè l'ideale nullo e l'ideale massimale). Di fatto, gli ideali non banali di A_P sono tutti e soli quelli del tipo $S^{-1}P^n$, con $n \geq 0$. Osserviamo anche che, siccome P è massimale in A, per la Proposizione 70 si ha $S^{-1}A/S^{-1}P \simeq A/P$.

Esempio 2. Sia A un anello artiniano, P un suo ideale primo e $M = S^{-1}P$ (con $S = A \setminus P$) l'unico ideale massimale della localizzazione A_P; P è massimale in A (perché A è artiniano) ed esiste $n \geq 1$ con $P^n = P^{n+1}$, inoltre (Lemma 45) P è il solo ideale primo di A contenuto in P. Quindi $A_P/M \simeq A/P$, e M è il solo ideale primo di A_P, di conseguenza (Proposizione 46) $M^n = (0)$ per qualche $n \geq 1$, minimo possibile. Ora, $S^{-1}P^n = S^{-1}P^{n+1}$ dunque $S^{-1}P^n = (0)$. Se, come al solito, f è l'omomorfismo da $A \to A_P$, dato da $f(a) = a/1$, si ha allora $P^n = \ker f$. Ora, A/P^n è un anello (artiniano) locale; si conclude quindi $A_P \simeq A/P^n$.

Esercizio 47. Sia P un ideale primo dell'anello A, e x un'indeterminata. Per il Lemma di Gauss (esercizio 9) $P[x]$ è un ideale primo di $A[x]$. Si dica se $A[x]_{P[x]}$ è isomorfo a $A_P[x]$.

Esercizio 48. [ex 3.5 in A.M.] Sa A un anello. Si assuma che per ogni ideale primo P di A, l'anello A_P non ha elementi nilpotenti $\neq 0$. Si provi che A non ha elementi nilpotenti $\neq 0$. È vero che se A_P è un dominio d'integrità, per ogni ideale primo P di A, allora A è un dominio d'integrità?

Esercizio 49. [ex 4.10 in A.M.] Sia P un ideale primo dell'anello A, $f : A \to A_P$ l'omomorfismo definito da $f(a) = a/1$ e $S_P = \ker f$. Si provino i seguenti fatti:

(i) $\sqrt{S_p} \subseteq P$;

(ii) $\sqrt{S_P} = P$ se e solo se P è minimale nell'insieme degli ideali primi di A;

(iii) se P' è un ideale primo di A con $P' \supseteq P$ allora $S_{P'} \subseteq S_P$.

4.3 Moduli frazionari.

[A.M. p. 38 e seguenti].

Mediante una procedura analoga a quella impiegata per l'anello A, si può 'frazionare' anche un qualsiasi A-modulo M. Per questo argomento, ci limitiamo ad esporre la costruzione e le definizioni, lasciando a chi legge tutte le dimostrazioni (che non dovrebbero porre problemi oltre eventualmente un poco di noia).
Dato S sottoinsieme moltiplicativamente chiuso di A, sull'insieme $M \times S$ si definisce la relazione $\simeq$ ponendo, per ogni $(a, x), (b, y) \in M \times S$,

$$(a, x) \simeq (b, y) \;\Leftrightarrow\; t \cdot (y \cdot a - x \cdot b) = 0 \text{ per qualche } t \in S.$$

Si provi che $\simeq$ è una relazione d'equivalenza su $M \times S$.
Denotata con m/s la classe di equivalenza di ciascun $(m, s) \in M \times S$, e posto $S^{-1}M$ l'insieme quoziente $S^{-1}M = \{m/s \mid (m, s) \in M \times S\}$, si definisca la somma su $S^{-1}M$,

$$m/s + m'/t = (t \cdot m + s \cdot m')/st$$

quindi un'azione di $S^{-1}A$ su $S^{-1}M$,

$$a/t \cdot m/s = (a \cdot m)/st.$$

(per ogni $m, m' \in M,\ s, t \in S,\ a \in A$); si provi che $S^{-1}M$ è in questo modo un $S^{-1}A$-modulo. In particolare, se P è un ideale primo di A e $S = A \setminus P$, si parla di $M_P = S^{-1}M$, visto come A_P-modulo, come della localizzazione in P del modulo M.

Come detto, enunciamo ora, sotto forma di esercizi, alcune tra le principali proprietà di questa costruzione.

Esercizio 50. [Prop. 3.3 di A.M.]. (1) Sia $\phi : N \to M$ un omomorfismo di A-moduli. Si provi che l'applicazione $S^{-1}\phi : S^{-1}N \to S^{-1}M$, data da $x/s \mapsto \phi(x)/s$ è ben definita ed è un omomorfismo di $S^{-1}A$-moduli (in particolare, se N è un A-sottomodulo di M allora $S^{-1}N$ è un $S^{-1}A$-sottomodulo di $S^{-1}M$).

(2) Siano $\phi : M \to N$ e $\psi : N \to L$ omomorfismi di A-moduli; si provi che

$$S^{-1}(\psi \circ \phi) = (S^{-1}\psi) \circ (S^{-1}\phi).$$

(3) Sia $0 \to N \xrightarrow{\nu} M \xrightarrow{\phi} L \to 0$ una sequenza esatta di A-moduli; si provi che $0 \to S^{-1}N \xrightarrow{S^{-1}\nu} S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}L \to 0$ una sequenza esatta di $S^{-1}A$-moduli.

Esercizio 51. [Corollary 3.4 in A.M.] Siano N, P sottomoduli del A-modulo M e sia S un sottoinsieme moltiplicativamente chiuso di A. Allora:

(1) $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$;

(2) $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$;

(3) $S^{-1}(M/N)$ e $S^{-1}(M)/S^{-1}(N)$ sono $S^{-1}(A)$-moduli isomorfi.

Esercizio 52. [Prop. 3.5 e 3.7 di A.M.]. Sia S un sottoinsieme moltiplicativamente chiuso dell'anello A e siano M, N du A- moduli. Allora:

(1) esiste un unico isomorfismo di $S^{-1}A$-moduli $f : S^{-1}A \otimes_A M \to S^{-1}M$ tale che $f((a/s) \otimes x) = ax/s$ per ogni $a/s \in S^{-1}A$ e $x \in M$;

(2) esiste un unico isomorfismo di $S^{-1}A$-moduli

$$f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \longrightarrow S^{-1}(M \otimes_A N)$$

tale che $f((x/s) \otimes (y/t)) = (x \otimes y)/st$ per ogni $x \in M$, $y \in N$ e $s, t \in S$.

Esercizio 53. [Prop. 3.8 in A.M.] Sia M un modulo per l'anello A. Si provi che sono equivalenti:

(1) $M = 0$;

(2) $M_P = 0$ per ogni ideale primo P di A;

(3) $M_J = 0$ per ogni ideale massimale J di A.

Esercizio 54. [ex. 3.14 in A.M.] Siano A un anello, I un ideale di A e M un A-modulo. Si provi che se $M_J = 0$ per ogni ideale massimale J di A tale che $J \supseteq I$, allora $M = IM$.

Soluzioni di alcuni esercizi.

Esercizio 45 – Soluzione. Siano $x/s \in S^{-1}I$ (con $x \in I, s \in S$) e $a/t \in S^{-1}A$;. Allora $st = 1 + y$ per qualche $y \in I$ e dunque $u = st - ax = 1 + y - ax \in 1 + I = S$. Quindi

$$1 - (x/s)(a/t) = (st - ax)/st = u/st$$

è invertibile in $S^{-1}A$. Per il Lemma 10, $x/s \in \mathrm{J}(S^{-1}A)$ ∎

Esercizio 46 – Soluzione. (1) Sia S sottoinsieme moltiplicativamente chiuso saturo di A. Dato $a \in A \setminus S$, allora per la saturazione di S, $(a) \cap S = \emptyset$. Dunque l'insieme Σ degli ideali I di A con $a \in I$ e $I \cap S = \emptyset$ non è vuoto: ordinato per inclusione è - come si vede facilmente - induttivo; dunque esiste un elemento M massimale in Σ; dato che $1 \in S$, $M \neq A$. Siano $x, y \in A \setminus M$; allora $M + (x) \notin \Sigma$, dunque esiste $s \in S \cap (M + (x))$, e similmente esiste $t \in S \cap (M + (y))$; se fosse, per assurdo, $xy \in M$ si avrebbe la contraddizione $st \in S \cap M$. Questo prova che M è un ideale primo, e dunque che $A \setminus S$ è unione di ideali primi. Viceversa, sia $S = A \setminus U$ dove U è unione di ideali primi di A. Che S sia un sottoinsieme moltiplicativamente chiuso è facile da vedere. Siano $x, y \in A$ con $x \notin S$; allora esiste un ideale $J \in U$ con $x \in J$, dunque $xy \in J_1$ e pertanto $xy \notin S$, il che dimostra che S è saturo.
L'ultima affermazione del punto (1) segue facilmente: se $S \subseteq A$ è moltiplicativamente chiuso e I ideale di A massimale tale che $S \cap I = \emptyset$ (poiché $0 \notin S$ l'ideale (0) ha intersezione vuota con S dunque - per Zorn - esistono ideali come questo I) allora, per stessa dimostrazione vista sopra, I è primo; si considera quindi l'unione U di tutti gli ideali (primi) di A che sono disgiunti da S, e si ottiene $\overline{S} = A \setminus U$.

(2) Sia $S = 1 + I$ con I ideale proprio di A; allora per ogni ideale proprio J con $I \subseteq J$ si ha $S \cap J = \emptyset$. Viceversa, sia P è un ideale massimale per essere contenuto in $A \setminus S$, e supponiamo, per assurdo $I \not\subseteq P$; allora $S \cap (P + I) \neq \emptyset$; esistono dunque $x, x' \in I, y \in P$ tali che $1 + x' = x + y$, ma allora $y = 1 + (x' - x) \in S$, assurdo. Quindi $I \subseteq P$. Per quanto visto al punto (1) si conclude quindi che $\overline{S} = A \setminus M$ dove M è l'unione di tutti gli ideali massimali contenenti I. ∎

Esercizio 49 – Soluzione. (i) Se $a \in \sqrt{S_P}$ e sia $n \geq 1$ tale che $a^n \in S_P$;. Allora $a^n/1 = 0/1$, dunque esiste $s \in A \setminus P$ con $a^n s = 0$; quindi, poiché P è primo, $a^n \in P$, cioè $a \in \sqrt{P} = P$.

(ii) Scriviamo $J = \sqrt{S_P}$. Supponiamo $J = P$; sia P' ideale primo di A con $P' \subseteq P$ e sia $a \in P$. Allora esiste $n \geq 1$ tale che $a^n/1 = 0$, ovvero $a^n s = 0$ per qualche $s \in A \setminus P \subseteq A \setminus P'$; quindi poiché P' è primo, $a^n \in P'$ e pertanto $a \in P'$, il che prova $P' = P$ e la minimalità di P nell'insieme degli ideali primi di A.

Viceversa, sia P minimale nell'insieme degli ideali primi di A, e $S = A \setminus P$; per la Proposizione 71, $M = S^{-1}P$ è l'unico ideale primo di A_P, dunque $S^{-1}P = \mathfrak{N}(A_P)$. Ne segue che per ogni $u \in P$ esiste $n \geq 1$ tale che $f(u^n) = u^n/1 = (u/1)^n = 0$, quindi $u \in \sqrt{S_P}$, provando l'identità $P = \sqrt{S_P}$.

(iii) Sia P' è un ideale primo di A con $P' \supseteq P$, e sia $S' = A \setminus P'$. Sia $u \in S_{P'}$; allora esiste $n \geq 1$ tale che $u^n/1 = 0$ in $A_{P'}$, cioeè esiste $t \in S'$ tale che $u^n t = 0$. Ma $S' \subseteq S$ e dunque $u^n/1 = 0$ in A_P, il che significa $u \in S_P$, provando l'inclusione desiderata. ∎

Esercizio 53 –Soluzione. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) è ovvia. Proviamo (iii) $\Rightarrow$ (i). Supposto $M \neq 0$, siano $0 \neq a \in M$ e $I = Ann_A(a)$. Allora, I è un ideale proprio di A, dunque esiste un ideale massimale J di A con $I \subseteq J$. Se fosse $M_J = 0$, allora in particolare $a/1 = 0$, quindi esiste $t \in A \setminus J$ tale che $0 = t \cdot (a - 0) = t \cdot a$, cioè $t \in Ann_A(a) \subseteq J$, che è assurdo. Quindi $M_J \neq 0$, e questo prova (iii) $\Rightarrow$ (i). ∎

Esercizio 54 – Soluzione. Applicare l'esercizio precedente ad M/IM come A/I-modulo. ∎

5 Dipendenza intera e valutazioni

[estratto dal capitolo 5 di A.M.]

5.1 Dipendenza intera.

Prima di entrare nel merito osserviamo che se A è un sottoanello dell'anello B, allora le operazioni in B definiscono su B stesso una struttura di A-modulo; come tale può essere finitamente generato oppure no, ma certamente è fedele, dato che $1_A = 1_B \in B$ e $Ann_A(1) = (0)$.

DEFINIZIONE. Sia A un sottoanello dell'anello B. Un elemento $b \in B$ si dice *intero* su A se esiste un polinomio *monico* $f \in A[x]$ tale che $f(b) = 0$, cioè se esistono $n \geq 1$ ed elementi $a_0, \ldots, a_{n-1}$ di A tali che

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0. \tag{15}$$

ESEMPIO. Sia $q = r/s \in \mathbb{Q}$, con $r, s \in \mathbb{Z}$, $s \geq 1$ e $(r, s) = 1$.Supponiamo q sia intero su $\mathbb{Z}$; allora esistono $n \geq 1$ e $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ tali che

$$q^n = \frac{r^n}{s^n} = \frac{a_{n-1}r^{n-1}}{s^{n-1}} + \cdots + \frac{a_1 r}{s} + a_0.$$

Moltiplicando per s^n: $r^n = a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n$; quindi s divide r^n e poiché r ed s sono coprimi, deve essre $s = 1$ e $q \in \mathbb{Z}$. Una dimostrazione analoga mostra he se B è il campo delle frazioni di un dominio a fattorizzazione unica D, allora gli elementi di B interi su D sono solo quelli di D stesso.

Ovviamente, ogni elemento di un anello A è intero su A; la prima domanda che naturalmente ci si pone è se l'insieme degli elementi di un sopranello B che sono interi su A costituisca un sottoanello di B. Vedremo che così è.

Proposizione 73. *Sia A un sottoanello dell'anello B, e sia $b \in B$, Le seguenti condizioni sono equivalenti,*

(1) *b è intero su A,*

(2) *$A[b]$ è un A-modulo finitamente generato;*

(3) *$A[b]$ è contenuto in un sottoanello C di B che è finitamente generato come A-modulo;*

(4) *esiste un $A[b]$-modulo fedele M che è finitamente generato come A-modulo.*

Dimostrazione. (1) $\Rightarrow$ (2). Se $b \in B$ è intero su A vale un'identità come in (15), ed allora si deduce facilmente che

$$A[b] = Ab^{n-1} + Ab^{n-2} + \cdots + Ab + A,$$

dunque $A[b]$ è finitamente generato come A-modulo.

(2) $\Rightarrow$ (3). Assumendo (2), basta prendere $C = A[b]$ per avere (3).

(3) $\Rightarrow$ (4). Assumendo (3), sia considera $M = C$. Poichè $A[b]$ è sottoanello di C, C è un $A[b]$-modulo, è finitamente generato come A-modulo per ipotesi, ed è fedele per quanto osservato all'inizio del capitolo.

(4) $\Rightarrow$ (1). Sia M come assunto in (4) e sia $u_1, \dots u_n$ un sistema di generatori per M come A-modulo. Allora, per ogni $1 \leq i \leq n$,

$$b \cdot u_i = \sum_{j=1}^{n} c_{ij} u_j$$

con $c_{ij} \in A$. Chiamiamo C la matrice $C = (c_{ij})$, indichiamo con I la matrice identica $n \times n$ (a coefficienti in A) e con $\underline{u}$ il vettore colonna $(u_1, \dots, u_n)^{\mathsf{T}}$; allora

$$(bI - C)\underline{u} = 0,$$

e, moltiplicando a sinistra per la matrice aggiunta di $bI - C$,

$$\det(bI - C)I\underline{u} = 0,$$

da cui segue $\det(bI - C) \cdot M = 0$. Quindi, per la fedeltà di M come $A[b]$-modulo, $\det(bI - C) = 0$, il che comporta che b è intero su A: il polinomio monico che si annulla in b è infatti $\det(xI - C)$. □

Diciamo che un anello B è *intero* su un suo sottoanello A se ogni elemento di B è intero su A.

Lemma 74. *Sia A un sottoanello dell'anello B, e siano $b_1, \dots, b_n \in B$ tali che b_1 è intero su A e, per $2 \leq i \leq n$, b_i è intero su $A[b_1, \dots, b_{i-1}]$. Allora $A[b_1, \dots b_n]$ è finitamente generato come A-modulo e, come anello, è intero su A.*

Dimostrazione. Per induzione su n. Se $n = 1$ l'affermazione segue dalla Proposizione 73. Sia $n \geq 2$; per ipotesi induttiva $A_1 = A[b_1, \dots b_{n-1}]$ è finitamente generato come A-modulo e, per il caso $n = 1$, $A[b_1, \dots, b_n]$ è finitamente generato come A_1-modulo. Risulta ora un semplice calcolo provare che, se $c_1, \dots c_k$ è un sistema di generatori di A_1 come A-modulo e $d_1, \dots, d_t$ un sistema di generatori di $A[b_1, \dots, b_n]$ come A_1-modulo,

allora l'insieme $\{c_i d_j \mid 1 \leq i \leq k, 1 \leq j \leq t\}$ è un sistema di generatori di $A[b_1, \ldots, b_n]$ come A-modulo.
Provato questo, l'implicazione (3) $\Rightarrow$ (1) della Proposizione 73, assicura che ogni elemento di $A[b_1, \ldots, b_n]$ è intero su A. □

Da ciò segue in particolare quello che volevamo.

Corollario 75. *Sia A un sottoanello dell'anello B; allora l'insieme*

$$\overline{A} = \{b \in B \mid b \text{ intero su } A\}$$

è un sottanello di B (contenente A), detto la chiusura intera *di A in B.*

Dimostrazione. Siano $b, c \in \overline{A}$; allora, per il Lemma 74, $A[b, c]$ è intero su A. In particolare $b - c$ e bc sono interi su A (cioè appartengono a $\overline{A}$). □

Sia A sottoanello di B. Diciamo che A è *integralmente chiuso* in B se $\overline{A} = A$.

Corollario 76. *Siano A, B, C anelli, con A sottoanello di B e B sottoanello di C; se C è intero su B e B è intero su A allora C è intero su A.*
In particolare, se A è sottoanello di B, $\overline{A}$ è integralmente chiuso in B.

Dimostrazione. Sia $c \in C$; per ipotesi esistono $b_0, \ldots, b_{n-1} \in B$ tali che

$$c^n = b_{n-1}c^{n-1} + \cdots + b_1 c + b_0.$$

Ma allora c è intero su $A[b_1, \ldots, b_{n-1}]$ (e ogni b_i è intero su A), quindi per il Lemma 74, $A[b_1, \ldots, b_{n-1}, c]$ è intero su A, in particolare c è intero su A. □

Definizione. Un dominio d'integrità si dice *integralmente chiuso* se coincide con la propria chiusura intera nel suo campo delle frazioni.

Esempio. L'anello $\mathbb{Z}$ e, più in generale, ogni dominio a fattorizzazione unica sono integralmente chiusi.

Esempio importante. Un numero complesso $z \in \mathbb{C}$ si dice *intero algebrico* se z è intero su $\mathbb{Z}$. Per il Corollario 75, l'insieme degli interi algebrici è un sottoanello di $\mathbb{C}$, ed interseca $\mathbb{Q}$ in $\mathbb{Z}$. Chiaramente, ogni radice di un numero intero è un intero algebrico.
Un *campo di numeri* è un sottocampo $\mathbb{K}$ del campo $\mathbb{C}$ dei numeri complessi tale che $[\mathbb{K} : \mathbb{Q}] < \infty$ (quindi $\mathbb{K}$ è contenuto nel campo dei numeri algebrici). Se $\mathbb{K}$ è un campo di numeri, la chiusura intera di $\mathbb{Z}$ in $\mathbb{K}$ si chiama *anello degli interi* di $\mathbb{K}$ e si denota con $\mathcal{O}_\mathbb{K}$. Quindi, $\mathcal{O}_\mathbb{K}$ è l'intersezione di $\mathbb{K}$ con l'anello degli interi algebrici.

Vogliamo ora descrivere gli anelli degli interi delle estensioni quadratiche:

$$\mathbb{K} = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\},$$

assumendo, cosa che chiaramente non è una vera limitazione, che $d \in \mathbb{Z}$ sia privo di quadrati (cioè non è diviso dal quadrato di alcun numero primo). $\mathbb{K}|\mathbb{Q}$ è un'estensione di Galois di grado 2 ed il suo gruppo di Galois è costituito dall'identità e dall'automorfismo γ definito da $\gamma(a + b\sqrt{d}) = a - b\sqrt{d}$.

Dati $a, b \in \mathbb{Q}$, supponiamo $z = a + b\sqrt{d}$ sia un intero algebrico, cioè $f(z) = 0$ per qualche polinomio monico $f \in \mathbb{Z}[x]$. Allora $0 = \gamma(f(z)) = f(\gamma(z))$ e dunque anche $\gamma(z) = a - b\sqrt{d}$ è un intero algebrico. Per il Corollario 75, si deduce che i numeri razionali $2a = z + \gamma(z)$ e $a^2 - b^2 d = z\gamma(z)$ sono interi algebrici; dunque $2a$, $a^2 - b^2 d$ appartengono a $\mathbb{Z}$. Viceversa, siano $a, b \in \mathbb{Q}$ tali che $2a$ e $a^2 - b^2 d$ appartengono a $\mathbb{Z}$; allora $z = a + b\sqrt{d}$ è un intero algebrico, in quanto radice del polinomio

$$(x - a)^2 - b^2 d = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Z}[x].$$

Abbiamo quindi stabilito che

$$\mathcal{O}_{\mathbb{K}} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q},\ 2a, a^2 - b^2 d \in \mathbb{Z}\}.$$

Osserviamo ora che se $2a, a^2 - b^2 d \in \mathbb{Z}$ allora

$$(2b)^2 d = (2a)^2 - 4(a^2 - b^2 d) \in \mathbb{Z},$$

e siccome $d \in Z$ è privo di quadrati, $2b \in \mathbb{Z}$. Abbiamo quindi che gli interi di $\mathbb{K}$ sono tutti e soli i numeri del tipo $u/2 + v/2\sqrt{d}$, con $u, v \in \mathbb{Z}$ e

$$\frac{u^2 - v^2 d}{4} \in \mathbb{Z},$$

cioè $u^2 - v^2 d \equiv 0 \pmod 4$. Distinguiamo ora due casi.

(i) $d \not\equiv 1 \pmod 4$. Allora, poichè 4 non divide d, u e v devono essere entrambi pari. Dunque

$$\mathcal{O}_{\mathbb{K}} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}].$$

(ii) $d \equiv 1 \pmod 4$. In questo caso, u, v sono entrambi pari o entrambi dispari, quindi

$$\frac{u}{2} + \frac{v}{2}\sqrt{d} = \frac{u - v}{2} + v\frac{1 + \sqrt{d}}{2}.$$

Quindi, in questo caso,

$$\mathcal{O}_{\mathbb{K}} = \Big\{a + b\frac{1 + \sqrt{d}}{2} \ \Big|\ a, b \in \mathbb{Z}\Big\} = \mathbb{Z}\Big[\frac{1 + \sqrt{d}}{2}\Big].$$

Ad esempio,

- l'anello degli interi di $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ è l'anello degli interi di Gauss $\mathbb{Z}[i]$;

- l'anello degli interi di $\mathbb{Q}(\sqrt{-5})$ è l'anello $\mathbb{Z}[\sqrt{-5}]$;
- l'anello degli interi di $\mathbb{Q}(\sqrt{5})$ è l'anello $\mathbb{Z}[(1+\sqrt{5})/2]$ (che contiene propriamente $\mathbb{Z}[\sqrt{5}]$).

Torniamo alla teoria generale e vediamo che la localizzazione si comporta bene rispetto alla chiusura intera.

Lemma 77. *Siano A, C sottoanelli dell'anello B , con $A \subseteq C$.*

(1) *Sia J un ideale di B; se C è intero su A allora $(C+J)/J$ è intero su $(A+J)/J$ in B/J.*

(2) *Sia S un sottoinsieme moltiplicativamente chiuso di A; se C è la chiusura intera di A in B allora $S^{-1}C$ è la chiusura intera di $S^{-1}A$ in $S^{-1}B$.*

Dimostrazione. (1) Questo discende piuttosto direttamente dalle definizioni ed è lasciato per esercizio.

(2) Sia $c/s \in S^{-1}C$, con $c \in C$ e $s \in S$. Poichè $c \in C$ è intero su A, $c^n = a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$, con $a_0, \ldots, a_{n-1} \in A$; ma allora

$$(c/s)^n = (a_{n-1}/s)(c/s)^{n-1} + \cdots + (a_1/s^{n-1})c/s + a_0/s^n,$$

e quindi c/s è intero su $S^{-1}A$.
Viceversa, sia $b/s \in S^{-1}B$ (con $b \in B$ e $s \in S$) intero su $S^{-1}A$. Allora, per un $n \geq 1$,

$$(b/s)^n = a_{n-1}/s_{n-1}(b/s)^{n-1} + \cdots + a_1/s_1(b/s) + a_0/s_0$$

con $a_0, \ldots, a_{n-1} \in A$ e $s_0, \ldots, s_{n-1} \in S$. Ora, $t = s_0 s_1 \cdots s_{n-1} \in S$, e moltiplicando l'identità di sopra per $(st)^n$ si ottiene

$$(bt)^n = y_{n-1}(bt)^{n-1} + \cdots + y_1(bt) + y_0$$

dove, per ogni $i = 0, \ldots, n_1$, $y_i = (a_i/s_i)t^n s^{n-i} \in A$. Quindi bt è intero su A, cioè $bt \in C$, e pertanto $b/s = bt/st \in S^{-1}C$. □

In particolare, se A è un dominio integralmente chiuso, allora tale è ogni sua localizzazione (questo segue anche dalle definizioni).

Proposizione 78. *Sia A un sottoanello del dominio d'integrità B e sia B intero su A. Allora B è un campo se e solo se A è un campo.*

Dimostrazione. Nelle ipotesi date, sia A un campo e $0 \neq b \in B$. Per ipotesi esistono $n \geq 1$, $a_0, \ldots, a_{n-1} \in A$ tali che

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0.$$

Scegliendo $n \geq 1$ il più piccolo possibile per aver una tale uguaglianza, poiché B è un dominio d'integrità si ha $a_0 \neq 0$. Quindi a_0 è invertibile in A, e se

$$c = a_0^{-1}(b^{n-1} - a_{n-1}b^{n-2} - \ldots - a_2 b - a_1),$$

si trova $bc = 1$. Quindi b è invertibile, e questo prova che B è un campo.
Viceversa, supponiamo B un campo e sia $0 \neq a \in A$. Allora $a^{-1} \in B$ dunque esistono $n \geq 1$, $a_0, \ldots, a_{n-1} \in A$, tali che

$$a^{-n} = a_{n-1}a^{-(n-1)} + \cdots + a_1 a^{-1} + a_0;$$

da cui

$$a^{-1} = a^{-n}a^{n-1} = a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1} \in A,$$

così provando che A è un campo. □

Corollario 79. *Siano A, B anelli, con $A \subseteq B$ e B intero su A. Allora, un ideale primo Q di B è ideale massimale se e solo se $Q \cap A$ è un ideale massimale di A.*

Dimostrazione. Sia $P = Q \cap A$. Per il punto (1) del Lemma 77, B/Q è intero su $(A+Q)/Q \simeq A/P$. Poiché Q è primo, B/Q (così come A/P) è un dominio d'integritá. Dalla Proposizione 78 segue quindi che P è massimale in A (cioè A/P è un campo) se e solo se Q è massimale in B. □

Teorema 80. *Sia A un sottoanello dell'anello B, con B intero su A. Per ogni ideale primo P di A esiste un ideale primo Q di B tale che $Q \cap A = P$.*

Dimostrazione. Per il punto (2) del Lemma 77, B_P è intero su A_P. Sia J un ideale massimale di B_P; allora, per il Corollario 79, $M = A_P \cap J$ è un ideale massimale di A_P, dunque è il suo unico ideale massimale. Se $f : B \to B_P$ è l'omomorfismo naturale $b \mapsto b/1$, e $g : A \to A_P$ l'omomorfismo $a \mapsto a/1$, allora $Q = f^{-1}(J)$ è un ideale primo di B e $Q \cap A = f^{-1}(J) \cap A = g^{-1}(M) = P$ □

Esempio. [ex. 5.4 in A.M.] Sia x un'indeterminata sul campo $\mathbb{K}$ e consideriamo gli anelli $A = \mathbb{K}[x^2 - 1]$ e $B = \mathbb{K}[x]$; chiaramente B è intero su A. Sia $Q = (x-1)$ ideale massimale di B; per il Corollario 79, $P = A \cap B$ è un ideale massimale di A. Tuttavia, B_Q non è intero su A_P (l'immersione di A_P in B_Q è ovvia, dato che $A \setminus P \subseteq B \setminus Q$); si provi infatti che l'elemento $1/(x+1) \in B_Q$ non è intero su A_P.

Esercizio 55. [ex. 5.5 in A.M.] Siano A, B anelli, con $A \subseteq B$ e B intero su A.

(1) Si provi che $A \cap U(B) = U(A)$.

(2) Si provi che $J(A) = J(B) \cap A$.

Esercizio 56. [ex. 5.7 in A.M.] Siano A un sottoanello dell'anello B tale che l'insieme $B \setminus A$ è chiuso per moltiplicazione. Si provi che A è integralmente chiuso in B.

Esercizio 57. [ex. 5.2 in A.M.] Sia A un sottoanello di B, con B intero su A, e sia $\phi : A \to \mathbb{K}$ un omomorfismo da A in un campo algebricamente chiuso $\mathbb{K}$. Si provi che ϕ si estende ad un omomorfismo $B \to \mathbb{K}$.

SOLUZIONE. Poiché $A/\ker(\phi) \simeq \phi(A)$, $P = \ker(\phi)$ è un ideale primo di A, quindi per il Teorema 80 esiste un ideale primo Q di B tale che $Q \cap A = P$. Ora, $\mathbb{K}$ contiene il campo delle frazioni $\mathbb{F}$ di A/P. Se F_1 è il campo delle frazioni di B/Q allora F_1 contiene il campo delle frazioni F di $A/P \simeq (A+Q)/Q$; ma anche $\mathbb{K}$ contiene una copia isomorfa di F e quindi, dato che F_1 è un'estensione algebrica di F, $\mathbb{K}$ contiene una copia isomorfa di F_1. (da scrivere meglio) ∎

Vediamo infine che la proprietà di essere integralmente chiuso è una proprietà locale; cioè una proprietà che è soddisfatta da un anello A (in questo caso, un dominio d'integrità) se e solo se vale in ogni sua localizzazione.

Proposizione 81. *Sia A un dominio d'integrità. Sono equivalenti:*

(1) *A è integralmente chiuso;*

(2) *A_P è integralmente chiuso per ogni ideale primo P di A;*

(3) *A_M è integralmente chiuso per ogni ideale massimale M di A.*

Dimostrazione. Sia $\mathbb{K}$ il campo delle frazioni di A e $\overline{A}$ la chiusura intera di A in $\mathbb{K}$. Sia P un ideale primo di A. Poiché A è un dominio d'integrità, A_P è un sottoanello di $\mathbb{K}$ (dunque $\mathbb{K}$ è il campo delle frazioni di A_P).
(1) $\Rightarrow$ (2). Per il Lemma 77, $S^{-1}\overline{A}$ (dove $S = A \setminus P$) è la chiusura intera di A_P in $\mathbb{K}$. Dunque, se A è integralmente chiuso (cioè $\overline{A} = A$) allora A_P è integralmente chiuso.
(2) $\Rightarrow$ (3) è ovvia.
(3) $\Rightarrow$ (1) Sia A_M è integralmente chiuso in K per ogni ideale massimale M di A. Sia $as^{-1} \in \mathbb{K}$ (con $a, s \in A$, $s \neq 0$) intero su A, allora s^{-1} è intero su A. Se, per assurdo, $s^{-1} \notin A$, esiste allora un ideale massimale J di A con $s \in J$; chiaramente s^{-1} è intero su A_J, dunque, per ipotesi, $s^{-1} \in A_J$, cioè $s^{-1} = bt^{-1}$ con $t \in A \setminus J$, che è assurdo perché $t = bs \in J$. Dunque s^{-1} (e as^{-1}) appartiene ad A. □

5.2 Anelli di valutazione

[seconda parte del capitolo 5 e estratti dal capitolo 9 di A.M.]

Sia A un dominio d'intergità e K il suo campo delle frazioni; A si dice un *anello di valutazione* se per ogni $0 \neq x \in K$ almeno uno tra x e x^{-1} appartiene a A.

Ad esempio, $\mathbb{Z}$ non è un anello di valutazione, mentre se p è un primo positivo la localizzazione $Z_{p\mathbb{Z}} = \{r/s \in \mathbb{Q} \mid p \text{ non divide } s\}$ è un anello di valutazione. Ogni campo è chiaramente un anello di valutazione.

Proposizione 82. *Sia A un anello di valutazione e K il suo campo delle frazioni:*

(1) *A è un anello locale;*

(2) *ogni sottoanello A' di K contenente A è un anello di valutazione;*

(3) *A è integralmente chiuso.*

Dimostrazione. (1) Per la Proposizione 7 è sufficiente provare che $M = A \setminus U(A)$ è un ideale di A. Sia $x \in M$, allora chiaramente $ax \in M$ per ogni $a \in A$. Resta da provare che $x + y \in M$ per ogni $x, y \in M$. Questo è ovvio se $x = 0$ oppure $y = 0$; possiamo quindi supporre $x \neq 0 \neq y$. Allora $x^{-1}y$ oppure $y^{-1}x = (x^{-1}y)^{-1}$ appartiene ad A; possiamo, senza perdere in generalità, assumere $x^{-1}y \in A$. Se, per assurdo, $x + y \notin M$, allora $(x + y)^{-1} \in A$ e

$$x^{-1} = x^{-1}(x + y)(x + y)^{-1} = (1 + x^{-1}y)(x + y)^{-1} \in A$$

che è assurdo. Dunque $x + y \in M$, e M è un ideale di A.

(2) È ovvio per definizione.

(3) Sia $b \in K$ intero su A; allora esistono $n \geq 1$ e $a_0, \ldots, a_{n-1} \in A$ tali che

$$b^n = a_{n-1}b^{n-1} + \cdots + a_1 b + a_0.$$

Proviamo, per induzione su n, che b appartiene ad A. Questo è banale se $n = 1$. Sia quindi $n \geq 2$ (e $b \neq 0$). Se $b^{-1} \notin A$ allora $b \in A$ per definizione di anello di valutazione. Se invece $b^{-1} \in A$ allora

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

e, poiché $a_1 + a_0 b^{-1} \in A$, concludiamo $b \in A$ per ipotesi induttiva. □

Valutazioni su un campo. Sia K un campo; un'applicazione suriettiva $\nu : K^* \to \mathbb{Z}$ si chiama una *valutazione discreta* su K se per ogni $x, y \in K^*$ sono soddisfatte le seguenti condizioni,

(i) $\nu(xy) = \nu(x) + \nu(y)$;

(ii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

È utile (ad esempio per non dover specificare ulteriori condizioni per la proprietà (ii)) estendere l'applicazione a tutto K ponendo $\nu(0) = \infty$.

Sia ν una valutazione discreta sul campo K; dalla proprietà (i) segue immediatamente $\nu(1) = 0 = \nu(-1)$ e, conseguentemente, $\nu(-x) = \nu(x)$ per ogni $x \in K^*$. Da ciò, per le proprietà (i) e (ii), si deduce che l'insieme

$$R_\nu = \{x \in K^* \mid \nu(x) \geq 0\} \cup \{0\}$$

è un sottoanello di K, detto *anello di valutazione di* ν. Da (i) si ha inoltre, per ogni $x \in K^*$, $\nu(x^{-1}) = \nu(1) - \nu(x) = -\nu(x)$, quindi R_v è un anello di valutazione.

Esempi importanti. 1) *Valutazione p-adica.* Sia p un primo positivo. Per ogni $z \in \mathbb{Z}$ definiamo $\nu_p(z)$ chiedendo che $p^{\nu_p(z)}$ sia la massima potenza di p che divide z. Se $q = \frac{n}{m} \in \mathbb{Q}^*$, con $n, m \in \mathbb{Z}$, si pone quindi

$$\nu_p(q) = \nu_p(n) - \nu_p(m)$$

(si osservi che ciò dipende solo dal numero q e non dalla particolare coppia (n, m) che lo rappresenti). Allora, la funzione $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$ è una valutazione discreta, detta la *valutazione p-adica* su $\mathbb{Q}$. L'anello di valutazione di ν_p è

$$\mathbb{Z}_{p\mathbb{Z}} = \{r/s \in \mathbb{Q} \mid p \text{ non divide } s\}.$$

2) *Analogo per polinomi.* K un campo, $\mathbb{K} = K(x)$ il campo delle frazioni algebriche su K, e $p \in K[x]$ un polinomio irriducibile. Ogni elemento $u \in \mathbb{K}^*$ si scrive in modo unico nella forma $u = p^z \frac{f}{g}$ con $z \in \mathbb{Z}$, $f, g \in K[x]$, $g \neq 0$ e $p \nmid f$, $p \nmid g$. Ponendo $\nu_p(u) = z$ risulta definita una valutazione discreta $\nu_p : \mathbb{K}^* \to \mathbb{Z}$. L'anello di valutazione è la localizzazione

$$K[x]_{(p)} = \{f/g \in K(x) \mid p \nmid g\}.$$

Osserviamo che anche la funzione su $K(x)^*$ ricavata dal grado: $\delta(f/g) = \deg(f) - \deg(g)$, è una valutazione discreta su $K(x)$. Si riconosce facilmente che δ è la valutazione $\nu_{x^{-1}}$, associata al polinomio irriducibile x^{-1} in $K(x^{-1}) = K(x)$.

Diciamo che un dominio d'integrità A è un *anello (o dominio) di valutazione discreta* se esiste una valutazione discreta ν sul suo campo delle frazioni tale che $R_\nu = A$. Per quanto osservato e per la Proposizione 82, un anello di valutazione discreta è un dominio locale integralmente chiuso.

Prima di descrivere altre proprietà generali degli anelli di valutazione discreta, ricordo che la dimensione, $\dim(A)$, di un anello A è l'estremo superiore delle lunghezze di catene di ideali primi di A. Se A è un dominio d'integrità, allora l'ideale (0) è primo, dunque

$\dim(A) = 0$ se e solo se A è un campo. Dunque, la prima generalizzazione consiste nei domini d'integrità di dimensione 1. Tenendo conto che ogni ideale proprio di un anello è contenuto in un ideale massimale (che è un ideale primo) si deduce immediatamente che: *un dominio d'integrità, che non sia un campo, ha dimensione* 1 *se e solo se ogni suo ideale primo non nullo è un ideale massimale.*

Proposizione 83. *Sia A un anello di valutazione discreta; allora A è noetheriano e* $\dim(A) = 1$.

Dimostrazione. Sia ν una valutazione discreta sul campo delle frazioni K di A. Sappiamo che A è locale e che $M = \{x \in \mathbb{K} \mid \nu(x) > 0\}$ è il suo unico ideale massimale. Siano $x, y \in A^*$ tali che $\nu(x) = \nu(y)$, allora $\nu(xy^{-1}) = 0$, dunque xy^{-1} è un elemento invertibile di A, e pertanto $(x) = (y)$ (ideali di A). Poichè ν è suriettiva, esiste $a \in A$ tale che $\nu(a) = 1$. Sia J un ideale proprio di A, e sia $n = \min\{\nu(x) \mid x \in J\}$, allora $1 \leq n = \nu(a^n)$, da cui per quanto osservato $J \subseteq (a^n)$. Ne segue che $M = (a)$ e che gli ideali propri e non nulli di A sono tutti e soli quelli nella catena discendente

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

Dunque A è noetheriano, e $\dim(A) = 1$, dato che il solo ideale primo del tipo (a^n) è $(a) = M$. □

Queste proprietà sono in una certa misura tipiche degli anelli di valutazione discreta, come mostra il seguente risultato.

Proposizione 84. *Sia A un dominio locale noetheriano di dimensione* 1*, sia M il suo unico ideale massimale e $\mathbb{K} = A/M$ il campo residuo. Sono equivalenti:*

(1) *A è un anello di valutazione discreta;*

(2) *A è integralmente chiuso;*

(3) *M è un ideale principale;*

(4) $\dim_{\mathbb{K}}(M/M^2) = 1$*;*

(5) *ogni ideale non-nullo di A è una potenza di M*

Dimostrazione. Osserviamo preliminarmente che se A, M e $\mathbb{K}$ sono come nelle ipotesi, allora M è l'unico ideale primo non-nullo di A. Se I è un ideale proprio e non-nullo di A, si ha quindi $M = \sqrt{I}$ e dunque dalla Proposizione 40 segue che $I \supseteq M^n$ per qualche intero $n \geq 1$.

(1) $\Rightarrow$ (2) segue dalla Proposizione 82.

(2) $\Rightarrow$ (3) Sia A integralmente chiuso. Sia $0 \neq a \in M$. Per quanto osservato esiste un minimo $n \geq 1$ tale che $M^n \subseteq (a)$; sia $b \in M^{n-1} \setminus (a)$ (si intende $M^0 = A$), e poniamo $x = ab^{-1}$, nel campo della frazioni di A. Ora, $x^{-1} \notin A$ (dato che $b \notin (a)$) dunque non è intero su A. Osserviamo che, per costruzione, $x^{-1}M$ è un ideale di A; se fosse $x^{-1}M \subseteq M$ allora M sarebbe un $A[x^{-1}]$–modulo fedele finitamente generato come A-modulo, quindi x^{-1} sarebbe intero su A per la Proposizione 73, che è assurdo; dunque $x^{-1}M = A$. Di conseguenza, $M = xA = (x)$.

(3) $\Rightarrow$ (4) Sia $M = (x)$ con $x \in A$. Allora $M^2 = (x^2)$; siccome $M \neq M^2$, si ha subito che, come $\mathbb{K}$-spazio vettoriale, M/M^2 è generato da $x + M^2$.

(4) $\Rightarrow$ (5) Sia $\dim_{\mathbb{K}}(M/M^2) = 1$. Sia J un ideale proprio e non-nullo di A; allora $J \supseteq M^n$, per qualche $n \geq 1$. Per i Lemmi 47 e 50, A/M^n è un anello artiniano ed ogni suo ideale è principale. Da ciò segue che J/M^n è una potenza di M/M^n e dunque che J è una potenza di M.

(5) $\Rightarrow$ (1) Poiché $M \neq M^2$ (in caso contrario, $M = (0)$ per il Lemma di Nakayama, e A non avrebbe dimensione 1), esiste $x \in M \setminus M^2$. Per ipotesi $(x) = M^n$ per qualche $n \geq 1$, quindi $(x) = M$. Segue che ogni ideale proprio non-nullo di A è del tipo (x^n) con $n \geq 1$. Per ogni elemento $0 \neq a \in A$ esiste dunque uno ed un solo intero $k \geq 1$ tale che $(a) = (x^k)$; poniamo $\nu(a) = k$. Posto K il campo delle frazioni di A, si definisce $\nu : K^* \to \mathbb{Z}$, ponendo, per ogni $a, b \in A,\ b \neq 0$, $\nu(ab^{-1}) = \nu(a) - \nu(b)$. Si verifica facilmente che ν è ben definita e che è una valutazione discreta su K il cui anello di valutazione è A. □

5.3 Domini di Dedekind.

Definizione. Un dominio d'integrità D si dice *dominio di Dedekind* se

(i) D è noetheriano;

(ii) D è integralmente chiuso;

(iii) $\dim(D) = 1$.

Per quanto visto, ogni anello di valutazione discreta è un dominio di Dedekind; di fatto, a norma della Proposizione 84, gli anelli di valutazione discreta sono esattamente i domini di Dedekind locali. Si osservi poi che, per la Proposizione 71, se D è un dominio di dimensione 1, allora ogni sua localizzazione ha anche dimensione 1; segue quindi dalla Proposizione 81 che un dominio noetheriano di dimensione 1 è un dominio di Dedekind se e solo se ogni sua localizzazione è un anello di valutazione discreta. L'anello degli interi $\mathbb{Z}$ è dominio di Dedekind non locale; vediamo altri esempi che suggeriscono la rilevanza di questa classe di anelli.

ESEMPI. 1) Ogni dominio a ideali principali (PID) è un dominio di Dedekind. Viceversa, si può provare che un dominio a fattorizzazione unica (UFD) è di Dedekind se e solo se è un PID.

2) Sia $\mathbb{K}$ un campo algebricamente chiuso e $f \in \mathbb{K}[x,y]$ un polinomio irriducibile; allora $D = \mathbb{K}[x,y]/(f)$ è un dominio di Dedekind.

Ci accontentiamo infine di enunciare, senza dimostrazioni, un paio di importanti risultati riguardanti i domini di Dedekind. Il primo è il seguente.

Teorema 85. *L'anello degli interi di un campo di numeri è un dominio di Dedekind.*

Il secondo riguarda la fattorizzazione degli ideali. Premettiamo un'osservazione più generale.

Proposizione 86. *Sia A un dominio noetheriano di dimensione 1. Allora ogni ideale non nullo di A si rappresenta in modo unico (a meno dell'ordine dei fattori) come prodotto di ideali primari i cui radicali sono a due a due distinti.*

Dimostrazione. Sia $I \neq (0)$ ideale del dominio noetheriano A. Per il Teorema 60, I ammette una decomposizione primaria irridondante: $I = \bigcap_{i=1}^n Q_i$, con i Q_i ideali primari tali che gli ideali primi $P_i = \sqrt{Q_i}$ sono tutti diversi. Poiché A è un dominio d'integrità e $\dim A = 1$, $P_1, \ldots, P_n$ sono ideali massimali distinti; sono quindi a due a due sono coprimi, cioè se $1 \leq i < j \leq n$, $P_i + P_j = A$. Da ciò segue che gli ideali Q_i ($1 \leq i \leq n$) sono a due a due coprimi: infatti, per la Proposizione 12, $\sqrt{Q_i + Q_j} = \sqrt{P_i + P_j} = A$ e dunque $Q_i + Q_j = A$. Si ha quindi

$$I = Q_1 \cap Q_2 \cap \ldots \cap Q_n = Q_1 Q_2 \cdots Q_n.$$

Supponiamo ora che $I = \prod_{i=1}^n Q_i'$, con Q_i' ideali primari i cui radicali sono a due a due distinti. Allora per lo stesso motivo di prima $I = \bigcap_{i=1}^n Q_i'$, e siccome gli ideali primi associati sono tutti isolati (essendo ideali massimali), per si ha $n = m$ e $\{Q_1', \ldots, Q_n'\} = \{Q_1, \ldots, Q_n\}$. □

Ideali frazionari. Sia D un dominio d'integrità e $\mathbb{K}$ il suo campo della frazioni. Un sottoinsieme J di $\mathbb{K}$ si dice *ideale frazionario* di D se J è un D-sottomodulo di $\mathbb{K}$ ed esiste $r \in D$ tale che $rJ \subseteq D$.

Lemma 87. *Siano D un dominio di Dedekind, $\mathbb{K}$ il suo campo delle frazioni e $(0) \neq I$ un ideale primo di D. Allora*

$$J = \{x \in \mathbb{K} \mid xI \subseteq D\}$$

è un ideale frazionario di D e $JI = D$.

L'ideale frazionario J, definito nell'enunciato precedente, associato all'ideale primo di I di D si denota con I^{-1}. Il risultato fondamentale per domini di Dedekind è il seguente.

Teorema 88. *Sia I un ideale frazionario del dominio di Dedekind D, allora esistono e a meno del loro ordine sono unici, numeri interi non nulli $k_1, \dots k_n$ ed ideali primi distinti $I_1, \dots, I_n$ di D tali che*

$$J = I_1^{k_1} I_2^{k_2} \cdots I_n^{k_n}.$$