Algebra 2

Giovanni Antonio Lucarelli

Queste dispense sono basate sulle lezioni del corso di Algebra 2 dell'Università di Pisa, anno accademico 2023/24, tenuto dai professori Enrico Sbarra e Andrea Bandini.

Indice

1 Anelli

1.1 Richiami di teoria degli anelli

Definizione. Un **anello** è un insieme A munito di due operazioni binarie $+ : A \times A \to A, \qquad \cdot : A \times A \to A$ tali che:

- $(A, +)$ è un gruppo abeliano;
- $\cdot$ è associativo: $\forall a, b, c \in A \ (ab)c = a(bc)$;
- il prodotto distribuisce sulla somma: $\forall a, b, c \in A$ $a(b + c) = ab + ac, \ (a + b)c = ac + bc$.

Se $\cdot$ è commutativo, ovvero $\forall a, b \in A \ ab = ba$, l'anello si dice **commutativo**; se $\exists 1 \in A$ tale che $\forall a \in A \ a \cdot 1 = 1 \cdot a = a$, l'anello è detto **unitario**, e 1 è detto **identità** di A. Da adesso in poi tutti gli anelli che considereremo saranno commutativi con identità, e saranno chiamati semplicemente "anelli".

Definizione. Siano A, B due anelli. Un **omomorfismo di anelli** è una funzione $f : A \to B$ tale che:

- $\forall a, b \in A \ f(a + b) = f(a) + f(b)$;
- $\forall a, b \in A \ f(ab) = f(a)f(b)$;
- $f(1_A) = 1_B$;

dove $1_A, 1_B$ sono rispettivamente l'identità di A e l'identità di B.

Esempio. *$id : A \to A$, $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $\varphi_a : A[x] \to A$, $\varphi_a(p(x)) = p(a)$, la valutazione di un polinomio in un elemento fissato $a \in A$.*

N.B.: Se $B \neq 0$, cioè se B non è l'anello banale con 1=0, $f : A \to B, f(a) = 0$ NON è un omomorfismo di anelli, poiché $f(1_A) = 0_B \neq 1_B$.

Sia A un anello. $B \subseteq A$ è un **sottoanello** se è un sottogruppo additivo di A, è chiuso per prodotto e $1 \in B$. $I \subseteq A$ è un **ideale** se è un sottogruppo additivo di A con la *proprietà di assorbimento*: $\forall i \in I, \ a \in A \ ai \in I$.
Se $S \subseteq A$, definiamo (S) come il più piccolo ideale che contiene S, ed è l'insieme di tutte le combinazioni lineari finite di elementi di S a coefficienti in A, ossia elementi della forma $\sum a_i s_i$ con $a_i \in A, s_i \in S$.
Se $S = a$, $(S) = (a)$ si dice ideale **principale**; se S è finito l'ideale (S) è **finitamente generato**.
Se I è un ideale di A, è possibile dotare l'insieme quoziente A/I di una struttura di anello: se $\pi : A \to A/I$ è la proiezione canonica al quoziente, e $\overline{a} = \pi(a)$ denota la classe laterale di a in A/I, si definisce $\overline{a} + \overline{b} = \overline{a + b}$, $\overline{a} \cdot \overline{b} = \overline{ab}$. Questa definizione rende π un omomorfismo.

Sia $f : A \to B$ un omomorfismo di anelli. Il **nucleo** (o *kernel*) di f è l'insieme $\ker(f) = \{a \in A \mid f(a) = 0\}$, ed è un ideale di A. L'**immagine** di f è l'insieme $\mathrm{Im}(f) = \{b \in B \mid \exists a \in A \text{ t.c. } f(a) = b\}$.

Richiamiamo anche i teoremi di omomorfismo per anelli:

Teorema 1.1 (1° teorema di omomorfismo)**.** Siano A, B due anelli, e $f : A \to B$ un omomorfismo. Sia inoltre $I \subseteq A$ un ideale con $I \subseteq \ker(f)$, e sia $\pi : A \to A/I$ la proiezione al quoziente. Allora $\exists!\ \overline{f} : A/I \to B$ tale che $\overline{f} \circ \pi = f$.

Da questo teorema si conclude che $A/\ker(f) \cong \mathrm{Im}(f)$.

Teorema 1.2 (2° teorema di omomorfismo)**.** Sia A un anello, e siano I, J due ideali di A con $I \subseteq J$. Allora J/I è un ideale di A/I e $(A/I)/(J/I) \cong A/J$.

La mappa $\pi : A \to A/J$, inoltre, induce una corrispondenza 1-1 tra gli ideali di A che contengono I e gli ideali di A/I, e tale corrispondenza preserva ideali primi e massimali ("teorema di corrispondenza").

Definizione. Sia A un anello. Lo **spettro** di A è definito come
$\mathrm{Spec}(A) = \{P \subseteq A \mid P \text{ è un ideale primo di } A\}$.
Si definisce inoltre $\mathrm{Max}(A) = \{m \subseteq A \mid m \text{ è un ideale massimale di } A\}$.

Ricordiamo che P è un ideale **primo** di A se $P \subsetneq A$ e $\forall a, b \in A$ tali che $ab \in P$, si ha $a \in P \vee b \in P$; m è un ideale **massimale** di A se $\forall I \supseteq m$ ideale, si ha $I = m \vee I = A$.

Inoltre P è primo se e solo se A/P è un dominio d'integrità ($1 \neq 0$ e $ab = 0 \iff a = 0 \vee b = 0$); m è massimale se e solo se A/m è un campo (ogni elemento diverso da 0 è invertibile), da cui si deduce che i massimali sono primi.

Sappiamo che ogni anello non banale ammette almeno un ideale massimale, e quindi almeno un ideale primo. Più in generale, ogni ideale proprio (in particolare, ogni elemento non invertibile) è contenuto in un ideale massimale.

Definizione (Dimensione di Krull)**.** Sia A un anello. La **dimensione di Krull** di A è l'estremo superiore della lunghezza di tutte le catene di ideali primi di A:

$$\dim(A) = \sup\{k \mid P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_k,\ P_i \in \mathrm{Spec}(A)\}.$$

Esempio.
1. *Se k è un campo, il suo unico ideale primo è (0), ed è massimale, quindi* $\dim(A) = 0$.
2. *Se $A = \mathbb{Z}$ (o un qualsiasi PID), i primi di A sono (0) e i massimali, quindi la catena più lunga è $(0) \subsetneq m$ per qualche ideale massimale m di A, e* $\dim(A) = 1$.

1.2 Operazioni tra ideali

Di seguito elenchiamo le più comuni operazioni tra ideali.

- Se $\{I_h\}_{h \in H}$ è una famiglia di ideali di un anello A (H è un insieme di indici), l'intersezione $\bigcap_{h \in H} I_h$ è un ideale di A.
- La somma $\sum_{h \in H} I_h$ è l'ideale generato dall'unione degli I_h, ovvero somme finite di elementi di $\bigcup_{h \in H} I_h$. In particolare, se I, J sono due ideali, $I + J = \{i + j \mid i \in I,\ j \in J\}$. In generale, l'unione $\bigcup_{h \in H} I_h$ non è un ideale, anzi, lo è se e solo se gli I_h sono annidati l'uno nell'altro.

- Se H è un insieme finito, il prodotto è l'ideale $\prod_{h=1}^{k} I_h = (\prod_{h=1}^{k} a_h \mid a_h \in I_h)$ (è necessario prendere l'ideale generato, altrimenti non ci sarebbe la chiusura per somma). Per $k \in \mathbb{N}$ poniamo $I^0 = A,\ I^1 = I,\ I^k = \prod_{h=1}^{k} I$.

- Il **quoziente**, o *colon*, è l'ideale $I : J = \{a \in A \mid aJ \subseteq I\}$, e $aJ \subseteq I$ significa $\forall j \in J\ aj \in I$. In particolare, se $I = 0$, definiamo l'**annullatore** di J come
$$\mathrm{Ann}(J) = 0 : J = \{a \in A \mid aj = 0\ \forall j \in J\}.$$

- Il **radicale** di I è $\sqrt{I} = \{a \in A \mid \exists k \in \mathbb{N} : a^k \in I\}$. Definiamo l'ideale dei **nilpotenti** (o **nilradicale**) di A come
$$\mathcal{N}(A) = \sqrt{(0)} = \{a \in A \mid \exists k \in \mathbb{N} : a^k = 0\}.$$

Esempio. *Sia $A = \mathbb{Z}$. Tutti i suoi ideali sono della forma (n) per qualche $n \in \mathbb{N}$. Abbiamo $(m) + (n) = (\gcd(m,n)),\ (m) \cap (n) = (\mathrm{lcm}(m,n)),\ (m)(n) = (mn),\ (m) : (n) = (\frac{m}{\gcd(m,n)})$. Mostriamo, per esempio, quest'ultima: sia $d = \gcd(m,n)$. Si ha $\frac{m}{d}an = a \cdot \frac{mn}{d} = a \cdot \mathrm{lcm}(m,n) \in (m)$. Quindi $(\frac{m}{d}) \subseteq (m) : (n)$. Viceversa, sia $a \in (m) : (n)$, vogliamo mostrare che $\frac{m}{d} | a$. Siccome $a \in (m) : (n)$, $\exists b \in \mathbb{Z} : an = bm = bd\frac{m}{d} \implies a = \frac{bd}{n}\frac{m}{d}$. Dunque basta mostrare che $\frac{n}{d} | b$. Infatti, si ha $\frac{n}{d} | a\frac{n}{d} = b\frac{m}{d}$, e poiché $\frac{m}{d}, \frac{n}{d}$ sono coprimi, si deve avere $\frac{n}{d} | b$, come voluto.*

Esempio. *Siano I, J, H ideali di A. Quali di queste proprietà valgono?*

1. $IJ \subseteq I \cap J$;
2. $IJ = I \cap J$;
3. $(I + J)(I \cap J) = IJ$;
4. $I \cap (J + H) = I \cap J + I \cap H$.

La 1. è vera: se $x = ij,\ i \in I,\ j \in J$, allora $ij \in I$ e $ij \in J$ poiché ij è multiplo sia di un elemento di I, sia di un elemento di J. Poiché gli x di questa forma generano IJ, anche $IJ \subseteq I \cap J$.

La 2. è falsa: sia $A = \mathbb{Z},\ I = J = (2)$. Allora $IJ = (4),\ I \cap J = (2)$, che sono diversi.

La 3. è falsa in generale: sia $A = k[x,y],\ I = (x),\ J = (y)$. Abbiamo $I+J = (x,y),\ IJ = I \cap J = (xy)$ (sono i multipli di x e di y, che sono irriducibili diversi e quindi coprimi, dunque i multipli di xy). Quindi $(I + J)(I \cap J) = (x,y)(xy) = (x^2y, xy^2) \neq (xy) = IJ$. In generale, vale il contenimento $\subseteq$: un generatore del membro di sinistra è della forma $(i+j)k,\ i \in I,\ j \in J,\ k \in I \cap J$. Si ottiene $(i+j)k = ik + jk$, e poiché $k \in I \cap J$, entrambi gli addendi (e quindi la loro somma) sono in IJ. L'uguaglianza vale se $A = \mathbb{Z}$ (o un PID): in tal caso, se $I = (m),\ J = (n),\ [(m) + (n)][(m) \cap (n)] = (\gcd(m,n))(\mathrm{lcm}(m,n)) =$

$(\gcd(m,n)\cdot\mathrm{lcm}(m,n)) = (mn) = (m)(n)$. *L'uguaglianza vale anche in anelli più generali, se* $I+J=A$ *(in tal caso diciamo che* I, J *sono comassimali): infatti,* $(I+J)(I\cap J) = I\cap J$*, dunque basta far vedere che* $I\cap J \subseteq IJ$*. Usando il fatto che* $1\in A,\ \exists i\in I,\ j\in J : i+j=1$*. Sia* $x\in I\cap J$*, allora* $x = x\cdot 1 = x(i+j) = xi+xj$*, e si conclude notando che entrambi gli addendi sono in* IJ*.*

La 4. è falsa in generale: sia $A = k[x,y],\ I = (x+y),\ J = (x),\ H = (y)$*.* $J+H = (x,y) \implies I\cap(J+H) = (x+y)$*, dato che* $I\subseteq J\cap H$*. Inoltre,* $I\cap J = (x(x+y)),\ I\cap H = (y(x+y))$ *(come prima, nelle intersezioni ci sono tutti i multipli di due polinomi coprimi, quindi i multipli del prodotto). Infine, se per assurdo* $x+y\in(I\cap J)+(I\cap H), \exists\alpha,\beta\in k[x,y] : \alpha x(x+y)+\beta y(x+y) = x+y \implies \alpha x+\beta y = 1$*, assurdo poiché* $(x,y)\subsetneq k[x,y]$*. In generale vale il contenimento* $\supseteq$*, visto che* $I\cap J, I\cap H\subseteq I\cap(J+H)$*. C'è uguaglianza se* $I\supseteq J$ *o* $I\supseteq H$*: senza perdere in generalità supponiamo* $I\supseteq J$*. Se* $x\in I\cap(J+H),\ \exists j\in J,\ h\in H : x = j+h$*, ma* $J\subseteq I \implies j\in I$*. Poiché* $x = j+h\in I$*, anche* $h\in I$*. Dunque* $j\in I\cap J(=J),\ h\in I\cap H \implies x = j+h\in(I\cap J)+(I\cap H)$*.*

Proposizione 1.3 (Proprietà del radicale)**.** Sia A un anello, I, J, H ideali di A.

1. Se $I\subseteq J,\ \sqrt{I}\subseteq\sqrt{J}$.
2. $I\subseteq\sqrt{I},\ \sqrt{\sqrt{I}} = \sqrt{I}$.
3. $\sqrt{IJ} = \sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J}$.
4. $\sqrt{I} = (1) \iff I = (1)$.
5. $\sqrt{I+J} = \sqrt{I+\sqrt{J}}$, ma in generale $\sqrt{I+J}\neq\sqrt{I}+\sqrt{J}$.
6. $\forall k\in\mathbb{N}\ \sqrt{I^k} = \sqrt{I}$.
7. $\sqrt{I+JH} = \sqrt{I+J}\cap\sqrt{I+H}$.

Osservazione. In generale $I+JH\subseteq(I+J)\cap(I+H)$, ma l'uguaglianza può non valere.

Dimostrazione. Dimostriamo, per esempio, la 3. e la 7. dando per buono le altre.

3. Mostriamo la seguente catena di inclusioni:

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

La prima segue dalla 1. e dal fatto che $IJ \subseteq I \cap J$. Per la seconda, preso $x \in \sqrt{I \cap J}$, $\exists n \in \mathbb{N} : x^n \in I \cap J \implies x \in \sqrt{I} \cap \sqrt{J}$. Per l'ultima, sia $x \in \sqrt{I} \cap \sqrt{J}$. $\exists m, n \in \mathbb{N} : x^m \in I,\ x^n \in J \implies x^{m+n} \in IJ \implies x \in \sqrt{IJ}$.

7. L'inclusione $\subseteq$ segue dall'osservazione e dalla 1. Per l'inclusione opposta, sia $x \in \sqrt{I+J} \cap \sqrt{I+H}$. Allora $\exists m, n \in \mathbb{N} : x^m \in I + J,\ x^n \in I + H$. Scriviamo $x^m = i_1 + j,\ x^n = i_2 + h$, con $i_1, i_2 \in I,\ j \in J,\ h \in H$. Si ha $x^{m+n} = (i_1 + j)(i_2 + h) = i_1 i_2 + i_1 h + i_2 j + jh \in I + JH$ poiché i primi tre addendi sono in I e l'ultimo in JH. Quindi $x \in \sqrt{I + JH}$.

□

1.3 Alcuni ideali speciali

Vogliamo studiare alcuni tipi di ideali speciali, che sono generalizzazioni degli ideali primi.

Definizione. Sia A un anello e I un ideale di A. Diciamo che I è:

- **radicale** se $\sqrt{I} = I$;
- **irriducibile** se non è l'intersezione di due ideali che lo contengono strettamente; scritto simbolicamente: $\forall I_1, I_2 \supsetneq I$ ideali di A, se $I_1 \cap I_2 = I$, allora $I_1 = I$ o $I_2 = I$;
- **primario** se $\forall x, y \in I$ tali che $xy \in I$ si ha $x \in I \vee y \in \sqrt{I}$.

Proposizione 1.4. Sia A un anello e I un suo ideale.

1. I è radicale se e solo se A/I è *ridotto* (un anello R si dice ridotto se $\mathcal{N}(R) = (0)$, ovvero se il suo unico nilpotente è 0;
2. I è primario se e solo se $\mathcal{D}(A/I) = \mathcal{N}(A/I)$. Qui $\mathcal{D}(R)$ denota l'insieme dei divisori di zero dell'anello R, quindi un ideale è primario se e solo se tutti i divisori di zero del quoziente sono nilpotenti.

Dimostrazione. 1. I è radicale $\iff \forall x \in A$ tale che $\exists n \in \mathbb{N} : x^n \in I \implies x \in I \iff \forall\ \overline{x} \in A/I$ tale che $\exists n \in \mathbb{N} : \overline{x}^n = \overline{0} \implies \overline{x} = \overline{0} \iff \mathcal{N}(A/I) = (0)$.

2. ($\Longleftarrow$) Siano $a, b \in A$ con $ab \in I,\ a \notin I$. In A/I abbiamo $\overline{0} = \overline{ab} = \overline{a}\overline{b}$, con $\overline{a} \neq \overline{0} \implies \overline{b} \in \mathcal{D}(A/I) = \mathcal{N}(A/I) \implies \overline{b}^n = \overline{0}$ per qualche $n \implies b^n \in I \implies b \in \sqrt{I} \implies I$ primario.

   ($\Longrightarrow$) Poiché tutti i nilpotenti sono divisori di zero, è sufficiente mostrare l'inclusione opposta. Se $\overline{a} \in \mathcal{D}(A/I)$, sia $\overline{b} \in A/I$ con $\overline{b} \neq \overline{0},\ \overline{ab} = \overline{0}$. In A si ottiene $ab \in I,\ b \notin I$, quindi, essendo I primario, $a^n \in I$ per qualche $n \implies \overline{a}^n = \overline{0} \implies \overline{a} \in \mathcal{N}(A/I)$.

□

Proposizione 1.5. Sia A un anello e P un suo ideale primo. Allora:

1. P è primario.
2. P è radicale.
3. P è irriducibile.

Dimostrazione. Dato che ogni dominio d'integrità è ridotto, e vale $\mathcal{D}(A/P) = \mathcal{N}(A/P) = (0)$, tutti gli ideali primi sono primari e radicali. Vediamo il terzo punto: siano $I, J \supsetneq P$ tali che $P = I \cap J$, e siano $i \in I \setminus P,\ j \in J \setminus P$. Siccome P è primo, $ij \notin P$, ma $ij \in IJ \subseteq I \cap J = P$, assurdo.

□

Proposizione 1.6. Sia A un anello e I un suo ideale proprio.

1. Se I è primario, $\sqrt{I}$ è primo.
2. Se $\sqrt{I}$ è *massimale*, I è primario.

Dimostrazione.

1. Siano $a, b \in A : ab \in \sqrt{I}$. Si ha $a^n b^n \in I$ per qualche n e, essendo I primario, o $a^n \in I$ o $b^{nk} \in I$ per qualche k, dunque $a \in \sqrt{I}$ o $b \in \sqrt{I}$, cioè $\sqrt{I}$ è primo.
2. Siano $a, b \in A : ab \in I$, e supponiamo $b \notin \sqrt{I}$. Si vuole mostrare che $a \in I$. Poiché $\sqrt{I}$ è massimale e $b \notin \sqrt{I}$, $(\sqrt{I}, b) = (1)$, ovvero si può scrivere $1 = m + cb,\ m \in \sqrt{I},\ c \in A$. Sia $n \in \mathbb{N}$ tale che $m^n \in I$. Allora $1 = (m + cb)^n = m^n + b\alpha$, per qualche $\alpha \in A$. Moltiplicando per a si ottiene $a = am^n + ab\alpha \in I$, poiché $m^n, ab \in I$.

□

Osservazione. Nel punto 2 l'ipotesi che $\sqrt{I}$ sia massimale è necessaria. Se supponiamo solo che $\sqrt{I}$ sia primo, la tesi può non valere. Infatti, sia $A = k[x, y],\ I = (x^2, xy)$. Abbiamo $\sqrt{I} = \sqrt{(x^2) + (xy)} = \sqrt{(x^2) + (x)(y)} = \sqrt{(x^2) + (x)} \cap \sqrt{(x^2) + (y)}$ (per la proposizione 1.1) $= \sqrt{(x)} \cap \sqrt{(x^2, y)} = (x) \cap (x, y) = (x)$. (x) è primo, ma non massimale, in quanto $A/(x) \cong k[y]$, che è un dominio ma non un campo. I ha dunque radicale primo, ma non è primario: infatti, in $A/(x^2, xy), \overline{y}$ è divisore di 0 in quanto $\overline{x} \neq \overline{0}$ e $\overline{xy} = \overline{0}$, ma non nilpotente, poiché nessuna potenza di y appartiene a I.

I prossimi risultati evidenziano il ruolo di primaria importanza degli ideali primi.

Proposizione 1.7. Sia A un anello. Il nilradicale di A è uguale all'intersezione di tutti gli ideali primi dell'anello, ossia

$$\mathcal{N}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$$

.

Dimostrazione. ($\subseteq$) Sia $x \in \mathcal{N}(A),\ \mathfrak{p} \in \mathrm{Spec}(A)$. Poiché $\exists n \in \mathbb{N} : x^n = 0$, e $0 \in \mathfrak{p}$, che è primo, $x \in \mathfrak{p}$. Per arbitrarietà di $\mathfrak{p}$ si ha il contenimento cercato.

($\supseteq$) Mostriamo che, se x non è nilpotente, c'è un ideale primo che non lo contiene. Sia $\Sigma = \{I \subseteq A \text{ ideale} \mid I \cap S = \emptyset\}$, dove $S = \{1, x, x^2, ...\}$ è l'insieme delle potenze di x. L'idea è di estrarre un elemento di Σ massimale per inclusione, e mostrare che tale elemento è un ideale primo. Per fare questo, però, bisogna verificare che Σ rispetti le ipotesi del lemma di Zorn. Innanzitutto, Σ è non vuoto poiché contiene l'ideale (0): infatti, (0) è disgiunto da S perché x non è nilpotente. Sia ora $C = \{I_\alpha\}_\alpha \subseteq \Sigma$ una catena (ovvero un sottoinsieme totalmente ordinato), e mostriamo che ha un maggiorante. Prendiamo $J = \bigcup_{I \in C} I$. J è un ideale in quanto unione di ideali in catena, ed è effettivamente in Σ poiché, se un elemento di S fosse in J, sarebbe in uno degli ideali di C, che contraddice la definizione di C. Quindi le ipotesi di Zorn sono soddisfatte, e C ammette un elemento massimale. Sia P un tale elemento massimale, e mostriamo che è primo. Osserviamo che P è ovviamente proprio, poiché $1 \in S$. Per assurdo, siano $a, b \notin P : ab \in P$. Allora gli ideali $(P, a),\ (P, b)$ contengono strettamente P, quindi per massimalità di P, non possono essere elementi della catena C. Dunque esistono $x^m, x^n \in S : x^m \in (P, a),\ x^n \in (P, b)$. Questo implica che $x^{m+n} \in (P, a)(P, b) \subseteq P$ (usando che $ab \in P$), ma $x^{m+n} \in S$, quindi $P \cap S \neq \emptyset$, assurdo visto che $P \in C$.

□

Osservazione. La stessa dimostrazione funziona sostituendo l'insieme delle potenze di x con un qualunque *sottoinsieme moltiplicativo* S di A, ovvero un sottoinsieme che contiene 1 ed è chiuso per prodotto.

Osservazione. La tecnica utilizzata per costruire P nella dimostrazione precedente è molto utile per costruire ideali primi con certe caratteristiche: in un certo senso, elementi massimali di famiglie di ideali (propri) hanno una "forte tendenza" a essere ideali primi.

La proposizione precedente ha un immediato corollario:

Corollario. Se I è un ideale di A, allora

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A),\ \mathfrak{p} \supseteq I} \mathfrak{p}$$

Dimostrazione. Sfruttando la corrispondenza tra ideali primi di A/I e ideali primi di A contenenti I, si ottiene: $x \in \sqrt{I} \iff x^n \in I \iff \overline{x}^n = 0 \iff \overline{x} \in \mathcal{N}(A/I) \iff \overline{x} \in P\ \forall P \in \mathrm{Spec}(A/I) \iff x \in \mathfrak{p}\ \forall\ \mathfrak{p} \supseteq I,\ \mathfrak{p} \in \mathrm{Spec}(A)$.

□

Abbiamo appena visto che intersecare tutti i primi dà l'ideale dei nilpotenti, quindi ci possiamo chiedere cosa succede se si intersecano gli ideali massimali.

Definizione (Radicale di Jacobson)**.** Il **radicale di Jacobson** di un anello A è l'intersezione di tutti i suoi ideali massimali:

$$J(A) = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}.$$

Si nota subito che, poiché tutti i massimali sono primi, $\mathcal{N}(A) \subseteq J(A)$.

C'è un modo semplice per testare se un elemento di A appartiene a $J(A)$, che sfrutta il seguente risultato:

Proposizione 1.8 (Caratterizzazione del radicale di Jacobson)**.** Sia A un anello. Allora $a \in J(A) \iff \forall b \in A\ 1 - ab$ è invertibile.

Dimostrazione. ($\Longleftarrow$) Sia $a \notin J(A)$, e sia $\mathfrak{m} \in \mathrm{Max}(A)$ tale che $a \notin \mathfrak{m}$. Allora $(\mathfrak{m}, a) = (1)$, quindi $1 = x + ab$ per qualche $x \in \mathfrak{m},\ b \in A \implies 1 - ab = x \in \mathfrak{m}$, dunque b è tale che $1 - ab \notin A^*$.

($\Longrightarrow$) Sia $a \in J(A)$, e per assurdo sia $b \in A$ tale che $1-ab$ non è invertibile. Allora $\exists \mathfrak{m}$ ideale massimale che contiene $1 - ab$. Poiché a è in tutti i massimali, appartiene anche a $\mathfrak{m}$, quindi $1 = (1 - ab) + ab \in \mathfrak{m}$, assurdo.

□

Esempio. *Se $A = \mathbb{Z}/(n)$ (o qualsiasi anello finito), $J(A) = \mathcal{N}(A)$: infatti, in un anello finito ogni ideale primo è massimale (l'anello quoziente è un dominio finito, quindi un campo).*

Esempio. *Se A è un anello, allora $J(A[x]) = \mathcal{N}(A[x])$. Il contenimento $\supseteq$ è banale, vediamo l'altro. Ci servono due lemmi preparatori.*

Lemma 1.9. $\mathcal{N}(A[x]) = \mathcal{N}(\mathcal{A})[x]$. Ovvero un polinomio è nilpotente se e solo se lo sono tutti i suoi coefficienti.

Dimostrazione. ($\supseteq$) Basta notare che, se $a \in \mathcal{N}(A),\ (ax^m)^n = 0$ per qualche n e per ogni m. Poiché $\mathcal{N}(A[x])$ è un ideale, tutte le somme di elementi di questo tipo (polinomi a coefficienti nilpotenti) sono a loro volta nilpotenti.

($\subseteq$) Sia $f = \sum_{k=0}^{n} a_k x^k \in \mathcal{N}(A[x])$. Allora $f^n = 0$ per qualche $n \in \mathbb{N}$. Il termine noto di f^n è a_0^n, che deve essere 0, quindi a_0 è nilpotente, e deve esserlo anche $f - a_0 = \sum_{k=1}^{n} a_k x^k$. $(f - a_0)^m = 0$ per qualche m, e il suo termine di grado minimo è $a_1 x$. Si deve avere $a_1^m x^m = 0$, quindi anche a_1 è nilpotente, e deve esserlo anche $f - a_0 - a_1 x$. Iterando il procedimento si ha la tesi.

□

Lemma 1.10. $f = \sum_{k=0}^{n} a_k x^k \in A[x]$ è invertibile se e solo se a_0 è invertibile e a_i è nilpotente $\forall i \geq 1$.

Dimostrazione. ($\Longleftarrow$) Sia $f = \sum_{k=0}^{n} a_k x^k$, con $a_0 \in A^*$ e $a_i \in \mathcal{N}(A)$ per ogni $i \geq 1$. Allora $f = a_0(1 + a_0^{-1} \sum_{k=1}^{n} a_k x^k) = a_0(1 - t)$. Qui $t = -a_0^{-1} \sum_{k=1}^{n} a_k x^k$ è nilpotente, in quanto $a_1, ..., a_n$ lo sono. Se $h \in \mathbb{N}$ è tale che $t^h = 0$, allora $(1-t)(1+t+t^2+\cdots+t^{h-1}) = 1 - t^h = 1$, e $a_0^{-1}(1+t+\cdots+t^{h-1})$ è l'inverso di f, ovvero f è invertibile.

($\implies$) Sia $f = \sum_{k=0}^{n} a_k x^k \in (A[x])^*$, con inverso $g = \sum_{j=0}^{m} b_j x^j$. Innanzitutto il termine noto di fg è $a_0 b_0 = 1$, quindi $a_0 \in A^*$. Per mostrare che a_i è nilpotente per ogni $i \geq 1$, facciamo vedere che a_i appartiene all'intersezione di tutti gli ideali primi di A. Sia $P \in \operatorname{Spec} A$: allora $A[x]/P[x] \cong (A/P)[x]$, e poiché $\overline{f}\overline{g} = \overline{1}$ in $(A/P)[x]$, $\overline{f} \in ((A/P)[x])^* = (A/P)^*$ (questo perché $(A/P)[x]$ è un dominio, dunque 1 può essere solo prodotto di costanti). Ma allora $a_1, ..., a_n$ si riducono a 0 modulo P, ovvero $a_i \in P \ \forall i \geq 1$. Poiché P è un primo arbitrario di A, gli a_i sono in tutti i primi di A, e quindi nilpotenti.

□

Ora mostriamo che ogni elemento di $J(A[x])$ è nilpotente. Se $f = \sum_{k=0}^{n} a_k x^k$ è in $J(A[x])$, per la caratterizzazione (1.8) $1 + xf = 1 + \sum_{k=1}^{n+1} a_{k-1} x^k \in A[x]^*$, quindi, per il lemma 1.10, tutti gli a_k sono nilpotenti, e per il lemma 1.9 f è nilpotente, come voluto.

Vediamo ora degli esempi di anelli in cui i nilpotenti e il Jacobson non coincidono. Lo troveremo facilmente in una classe di anelli molto importante, che sarà studiata in modo approfondito nel resto del corso.

Definizione (Anello locale)**.** $(A, \mathfrak{m})$ si dice **anello locale** se $\mathfrak{m}$ è l'unico ideale massimale di A. $A/\mathfrak{m}$ è detto **campo residuo**.

Esempio. *Se p è un numero primo e $n \in \mathbb{N}$, $\mathbb{Z}/(p^n)$ è un anello locale: infatti, se I è massimale in $\mathbb{Z}/(p^n)$, deve corrispondere a un massimale di $\mathbb{Z}$ che contiene (p^n), quindi $p \in I$, dato che I è primo. Si conclude che I è necessariamente l'ideale massimale corrispondente a $(p) \subseteq \mathbb{Z}$.*

Anche gli anelli hanno una caratterizzazione abbastanza semplice:

Proposizione 1.11 (Caratterizzazione degli anelli locali)**.** Sia A un anello.

1. Se $\mathfrak{m}$ è un ideale proprio tale che $A \setminus \mathfrak{m} = A^*$, allora $(A, \mathfrak{m})$ è locale.
2. Se $\mathfrak{m}$ è massimale e $1 + a \in A^* \ \forall a \in A$, allora $(A, \mathfrak{m})$ è locale.

Dimostrazione.
1. Sia I un ideale proprio di A. I non ha elementi invertibili, quindi è contenuto in $\mathfrak{m}$. Dunque $\mathfrak{m}$ è l'unico ideale massimale di A.
2. Usiamo il punto 1. Sia $b \notin \mathfrak{m}$. Allora $(\mathfrak{m}, b) = (1)$ e si può scrivere $1 = a + bc,\ a \in \mathfrak{m},\ c \in A$. Dunque $bc = 1 - a$, che è invertibile per ipotesi, quindi anche b è invertibile e si conclude per il punto precedente.

□

Ovviamente, se $(A, \mathfrak{m})$ è un anello locale, $J(A) = \mathfrak{m}$, quindi, se A ha altri primi oltre a $\mathfrak{m}$, $\mathcal{N}(A) \neq J(A)$.

Esempio. *Sia K un campo, e consideriamo $A = K[[x]]$, l'anello delle serie di potenze formali nell'indeterminata x. Mostriamo che A è locale, con ideale massimale (x). Innanzitutto, (x) è massimale, poiché $K[[x]]/(x) \cong K$. Per la caratterizzazione degli anelli locali, ci basta mostrare che $f = 1 + xh \in A^* \ \forall h$, dove $h = \sum_{k\geq 0} a_k x^k$. Questo equivale a mostrare che tutte le serie $f = \sum_{k\geq 0} a_k x^k$ con termine noto $a_0 = 1$ sono invertibili. Costruiamo induttivamente la serie $g = \sum_{k\geq 0} b_k x^k$ tale che $fg = 1$. Ovviamente $b_0 = 1$ in quanto il termine noto di fg è $a_0 b_0$. Supponiamo di aver trovato i coefficienti $b_0, b_1, ..., b_{n-1}$, e troviamo b_n. Il coefficiente di x^n in fg è $\sum_{k=0}^{n} a_k b_{n-k}$, che deve essere uguale a 0. Isolando l'incognita b_n e ricordando che $a_0 = 1$, si ottiene $b_n = -\sum_{k=1}^{n} a_k b_{n-k}$. Dunque questa scelta dei b_n dà l'inversa di f in A, e quindi $(K[[x]], (x))$ è locale.*

In $A = K[[x]]$, $J(A) = (x)$, $\mathcal{N}(A) = (0)$ (è un dominio).

Esempio. *Sia p un numero primo, e sia $A = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid b \not\equiv 0 \mod p\}$. Per semplicità consideriamo solo frazioni ridotte ai minimi termini. È un sottoanello di $\mathbb{Q}$, in quanto sommando e moltiplicando elementi di A il denominatore del risultato è il prodotto dei denominatori, e il prodotto di numeri non multipli di p non è multiplo di p. Mostriamo che A è un anello locale con ideale massimale $I = \{\frac{a}{b} \in A \mid a \equiv 0 \mod p\}$.*

Sia $f : \mathbb{Z}_{(p)} \to \mathbb{Z}/(p)$, $f(\frac{a}{b}) = ab^{-1} \mod p$. È un omomorfismo di anelli surgettivo $[\mathbb{Z}/(p) \ni x = f(\frac{x}{1})]$ con nucleo I ($ab^{-1} \equiv 0 \mod p \iff a \equiv 0 \mod p$). Dunque $\mathbb{Z}_{(p)}/I \cong \mathbb{Z}/(p)$, il campo con p elementi, che implica che I è un ideale massimale. Per vedere che è locale, basta notare che, se $\frac{a}{b} \notin I$, $a \not\equiv 0 \mod p$ e quindi $\frac{b}{a} = (\frac{a}{b})^{-1} \in \mathbb{Z}_{(p)}$. Abbiamo che tutti gli elementi fuori da I sono invertibili, cioè che A è locale, con ideale massimale I e campo residuo isomorfo a $\mathbb{Z}/(p)$. Anche qui $J(A) \neq \mathcal{N}(A)$: $J(A) = I$, $\mathcal{N}(A) = (0)$, essendo A un dominio.

Si può generalizzare quest'ultimo esempio: siano $\{p_1, ..., p_k\}$ numeri primi, e sia $A = \mathbb{Z}_{(p_1,...,p_k)} = \{\frac{a}{b} \in \mathbb{Q} \mid b \not\equiv 0 \mod p_i \ \forall i\}$. Procedendo in modo simile a prima, si dimostra che è un sottoanello di $\mathbb{Q}$ e che $I_j = \{\frac{a}{b} \in A \mid p_j | \ a\}$ è un ideale massimale di A per ogni j. In realtà questi sono i soli ideali massimali di A, dunque A ha un numero finito di ideali massimali. (Un anello con questa proprietà è detto *semilocale*). Per dimostrare questo fatto, prendiamo I massimale non contenuto in nessuno degli I_j. Vorremmo trovare un elemento x di I che non appartiene a *nessun* I_j, cioè un elemento di $I \setminus \bigcup_{j=1}^{k} I_j$. Infatti un tale x avrebbe numeratore non divisibile per nessuno dei p_j, e quindi il suo inverso in $\mathbb{Q}$ sarebbe un elemento di A, ovvero x è un'unità in A e $I = A$, assurdo. Ora, se gli I_j sono ideali generici, non necessariamente è possibile trovare x con la proprietà cercata, ma si può fare nel caso in cui gli I_j sono *primi*, come nel nostro caso. Questo fatto è noto come *lemma di scansamento* (o *prime avoidance*):

Proposizione 1.12 (Lemma di scansamento)**.** Sia A un anello, I un ideale di A e $\{P_1, ..., P_k\}$ ideali primi tali che $I \subseteq \bigcup_{j=1}^{k} P_j$. Allora $\exists i_0$ tale che $I \subseteq P_{i_0}$.

Dimostrazione. Mostriamo che se $\forall j\ I \not\subseteq P_j$, allora $I \not\subseteq \bigcup_{j=1}^{k} P_j$, procedendo per induzione su n.

Passo base, $k = 1$: ovvio.

Passo induttivo, $k-1 \implies k$: per ipotesi induttiva, $\forall i\ \exists a_i \in I \setminus \bigcup_{j=1,\ j\neq i}^{k} P_j$. Ci sono due casi:

1. se $a_i \notin P_i$ per qualche i, abbiamo finito;
2. $a_i \in P_i\ \forall i$: consideriamo $x = a_1 + a_2a_3...a_k$. Poiché $a_i \in I\ \forall i,\ x \in I$. Se $x \in P_i$ per qualche $i > 1$, dato che anche $a_2a_3...a_k$ appartiene a P_i, in quanto multiplo di a_i, si avrebbe $a_1 \in P_i$, contraddizione. Resta da mostrare che $x \notin P_1$: se così non fosse, essendo $a_1 \in P_1$, avremmo anche $a_2a_3...a_k \in P_1$, che è assurdo poiché $a_i \notin P_1\ \forall i > 1$ e P_1 è primo.

□

Proposizione 1.13. Sia P un ideale primo e $I_1, ..., I_n$ ideali di A. Allora:

- se $P \supseteq \prod_{k=1}^{n} I_k$, allora $P \supseteq I_k$ per qualche k;
- se $P \supseteq \bigcap_{k=1}^{n} I_k$, allora $P \supseteq I_k$ per qualche k.

Dimostrazione.

- Se per assurdo $I_k \not\subseteq P$ per ogni k, sia $a_k \in I_k \setminus P$ per ogni k. Allora $a_1a_2 \cdots a_n \in \prod_{k=1}^{n} I_k$, ma non appartiene a P, in quanto nessun a_k è in P e P è primo, contraddicendo l'ipotesi.
- Basta osservare che $P \supseteq \bigcap_{k=1}^{n} I_k \supseteq \prod_{k=1}^{n} I_k$, e applicare quanto appena dimostrato.

□

1.4 Estensione e contrazione di ideali

Apriamo questa sezione con un esempio che motiverà i prossimi risultati.

Sia A un anello e I un suo ideale. Consideriamo $I[x] = \{\sum a_i x^i \mid a_i \in I\}$ l'insieme dei polinomi a coefficienti in I. Si verifica facilmente che è un ideale di $A[x]$. Consideriamo l'inclusione naturale $\varphi : A \hookrightarrow A[x]$ e la proiezione canonica $\pi : A[x] \to A[x]/I[x]$. Poiché $\ker(\pi \circ \varphi) = I[x] \cap A = I$, c'è un omomorfismo iniettivo da A/I in $A[x]/I[x]$. Se $I[x]$ è primo, $A[x]/I[x]$ è un dominio, quindi anche A/I è un dominio e I è primo. D'altro canto, c'è una mappa naturale

$f : A[x] \to (A/I)[x],\ f(\sum a_i x^i) = \sum \overline{a_i} x^i$, che riduce tutti i coefficienti modulo I. Tale mappa è chiaramente surgettiva e ha nucleo $I[x]$ (si devono annullare tutti i coefficienti dell'immagine, e questo accade solo se provengono da I). Dunque $A[x]/I[x] \cong (A/I)[x]$. Se I è primo, A/I è un dominio, quindi $(A/I)[x]$ è un dominio, ed è isomorfo a $A[x]/I[x]$, quindi $I[x]$ è primo in $A[x]$. Abbiamo dunque dimostrato che I è un primo di A se e solo se $I[x]$ è un primo di $A[x]$.

Vogliamo ora studiare come si trasportano le proprietà degli ideali tramite omomorfismi.

Definizione (Estensione e contrazione)**.** Siano A, B due anelli, e sia $\varphi : A \to B$ un omomorfismo. Se I è un ideale di A, l'**estensione** di I in B tramite φ è l'ideale generato dall'immagine di I in B: $I^e = (\varphi(I))$. Se J è un ideale di B, la **contrazione** di J in A tramite φ è la controimmagine di J: $J^c = \varphi^{-1}(J) = \{a \in A \mid \varphi(a) \in J\}$.

Osservazione. In generale $\varphi(I)$ NON è un ideale! Basta pensare all'inclusione di $\mathbb{Z}$ in $\mathbb{Q}$: l'immagine di qualsiasi ideale non nullo non è un ideale in $\mathbb{Q}$.

Le operazioni di estensione e contrazione godono delle seguenti proprietà:

1. Se I è un ideale di A, I^e è un ideale di B; se J è un ideale di B, J^c è un ideale di A;
2. Se $I_1 \subseteq I_2,\ I_1^e \subseteq I_2^e$; se $J_1 \subseteq J_2,\ J_1^c \subseteq J_2^c$;
3. $I \subseteq I^{ec}$, $J \supseteq J^{ce}$;
4. $I^{ece} = I^e,\ J^{cec} = J^c$.

Dimostrazione. Mostriamo la 3 e la 4.

3. Se $i \in I,\ \varphi(i) \in I^e$ e quindi $i \in I^{ec}$. J^c è l'insieme degli elementi di A che vanno a finire in J, quindi $\varphi(J^c) \subseteq J$. Poiché J è un ideale, si ha anche $J^{ce} = (\varphi(J^c)) \subseteq J$.

4. In entrambi i casi un'inclusione segue dalla 2 e dalla 3. Rimane da mostrare che $I^{ece} \subseteq I^e,\ J^{cec} \supseteq J^c$: facciamolo per la prima. I^{ec} è l'insieme degli elementi di A la cui immagine è in I^e, quindi $\varphi(I^{ec}) \subseteq I^e$, che è un ideale, quindi $I^{ece} = (\varphi(I^{ec})) \subseteq I^e$.

□

Diamo un controesempio all'uguaglianza nel punto 3: prendiamo $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ l'inclusione, $I = (2)$. Allora $I^{ec} = \mathbb{Z}$, in quanto l'estensione di I contiene 2, che è un'unità in $\mathbb{Q}$. Consideriamo ora $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$, e sia $J = (x)$. Allora $J^{ce} = (0)$, visto che $J^c = (0)$ e, chiaramente, $(0)^e = (0)$. (Invece $(0)^c = \ker(\varphi)$).

In generale la contrazione tende a comportarsi meglio dell'estensione: consideriamo $A \xrightarrow{\varphi} B \xrightarrow{\pi} B/J$. Il nucleo della composizione è J^c, quindi c'è un omomorfismo iniettivo da A/J^c in B/J. Questo implica che ogni proprietà di un anello che è ereditata dai suoi sottoanelli corrisponde a una proprietà ereditata dalla contrazione di un ideale: per esempio, sottoanelli di domini sono domini, quindi, se J è primo, J^c è primo; sottoanelli di anelli ridotti sono ridotti,

quindi contrazioni di ideali radicali sono ancora radicali; se in un anello tutti i divisori di zero sono nilpotenti, lo stesso vale per qualunque suo sottoanello, quindi contrazioni di ideali primari sono ancora primari. Invece, sottoanelli di un campo non sono necessariamente campi, dunque, se J è massimale, J^c può non essere massimale: per esempio, presa l'inclusione di $\mathbb{Z}$ in $\mathbb{Q}$, (0) è massimale in $\mathbb{Q}$, ma $(0)^c = (0)$ non è massimale in $\mathbb{Z}$.

L'estensione non si comporta altrettanto bene: sia $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, e sia $I = (p)$, dove p è un numero primo tale che $p \equiv 1 \mod 4$. Da un risultato di teoria dei numeri p è somma di due quadrati, $p = a^2 + b^2$, che negli interi di Gauss si fattorizza come $(a+ib)(a-ib)$. Quindi $(p)^e = (a+ib)(a-ib)$, e si può mostrare (ad esempio con il teorema cinese del resto) che $\mathbb{Z}[i]/(p)^e \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$, che ha divisori di zero non nilpotenti. Dunque $(p) \subseteq \mathbb{Z}$ è massimale, ma $(p)^e \subseteq \mathbb{Z}[i]$ non è nemmeno primario. Se invece prendiamo $J = (2)$, $2 = i(1-i)^2$, quindi $(2)^e = (1-i)^2$, che non è un ideale radicale.

Le cose funzionano molto meglio se φ è *surgettivo*.

Teorema 1.14. Siano A, B due anelli, $\varphi : A \to B$ un omomorfismo di anelli surgettivo. Allora:

1. Se I è un ideale di A, $I^e = \varphi(I)$, cioè $\varphi(I)$ è un ideale di B.
2. $I^{ec} = I + \ker(\varphi)$, $J^{ce} = J$.
3. C'è una corrispondenza biunivoca tra ideali di A che contengono $\ker(\varphi)$ e ideali di B, e tale corrispondenza preserva gli ideali primi, massimali, radicali e primari.

Dimostrazione.

1. Sappiamo già che l'immagine di un ideale è un sottogruppo additivo di B, resta da dimostrare la proprietà di assorbimento. Sia $b \in B$, $j \in \varphi(I)$. Poiché φ è surgettivo, $\exists a \in A$, $i \in I : \varphi(a) = b$, $\varphi(i) = j$. Dunque $\varphi(ai) = bj \in \varphi(I)$, in quanto $ai \in I$.

2. Dalle proprietà di estensione e contrazione si ha $I^{ec} \supseteq I$, e la contrazione di qualunque ideale di B contiene $\ker(\varphi)$. Per l'inclusione opposta, sia $x \in I^{ec}$. Allora $\varphi(x) \in I^e = \varphi(I) \implies \exists y \in I : \varphi(x) = \varphi(y) \implies x - y \in \ker(\varphi)$. Quindi $x = y + (x - y) \in I + \ker(\varphi)$. Per mostrare che $J^{ce} = J$, osserviamo che $J^{ce} = \varphi(J^c) = \varphi(\varphi^{-1}(J)) = J$ per la surgettività di φ.

3. La corrispondenza biunivoca viene dal punto 2: infatti, se I è un ideale di A che contiene $\ker(\varphi)$, $I^{ec} = I + \ker(\varphi) = I$, e se J è un ideale di B, $J^c \supseteq \ker(\varphi)$, e $J^{ce} = J$. Dunque estensione e contrazione sono una l'inversa dell'altra, e inducono una corrispondenza biunivoca tra l'insieme degli ideali di A contenenti $\ker(\varphi)$ e l'insieme degli ideali di B. Consideriamo le mappe $A \xrightarrow{\varphi} B \xrightarrow{\pi} B/J$. $\pi \circ \varphi$ è surgettiva in quanto composizione di mappe surgettive, e il suo nucleo è J^c. Si deduce che $A/J^c \cong B/J$. Se B/J è un dominio, o un campo, o ridotto, o ha divisori di zero nilpotenti, anche A/J^c ha la stessa proprietà, quindi, se J è primo, massimale, radicale o primario, anche J^c lo è. Viceversa, se I è un ideale di A contenente $\ker(\varphi)$,

consideriamo $A \xrightarrow{\varphi} B \xrightarrow{\pi} B/I^e$. Ragionando come sopra, e usando il fatto che $\ker(\pi \circ \varphi) = I^{ec} = I$, si ottiene $A/I \cong B/I^e$, dunque se I è primo, massimale, radicale o primario, anche I^e lo è.

□

Vediamo come estensione e contrazione si comportano rispetto a somma, prodotto e intersezione:

1. $(I_1 + I_2)^e = I_1^e + I_2^e$;
2. $(I_1 I_2)^e = I_1^e I_2^e$;
3. $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$;
4. $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$;
5. $(J_1 J_2)^c \supseteq J_1^c J_2^c$;
6. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

Mostriamo la 1, e dei controesempi alle uguaglianze per 3, 4, 5.

1. $(\subseteq)$ Un generatore del membro sinistro è della forma $\varphi(i_1 + i_2)$, con $i_1 \in I_1,\ i_2 \in I_2$. Ma $\varphi(i_1 + i_2) = \varphi(i_1) + \varphi(i_2) \in I_1^e + I_2^e$.

$(\supseteq)$ $I_1, I_2 \subseteq I_1 + I_2 \implies I_1^e, I_2^e \subseteq (I_1 + I_2)^e \implies I_1^e + I_2^e \subseteq (I_1^e + I_2)^e$.

3. Sia $f : \mathbb{Z}[x, y] \to \mathbb{Z},\ f(x) = 6,\ f(y) = 21$, esteso a un omomorfismo, e siano $I_1 = (x),\ I_2 = (y)$. $(I_1 \cap I_2)^e = (xy)^e = (f(xy)) = (126)$, ma $I_1^e \cap I_2^e = (f(x)) \cap (f(y)) = (6) \cap (21) = (42)$.

4. Sia $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ l'inclusione ovvia, siano $J_1 = (2+i),\ J_2 = (2-i)$. Allora $J_1^c = J_2^c = (5) \implies J_1^c + J_2^c = (5)$, ma $J_1 + J_2 = (1)$, e $(J_1 + J_2)^c = (1)$.

5. Sia i come nel controesempio a 4, e siano $J_1 = J_2 = (1 - i)$. Si ha $J_1^c = J_2^c = (2)$ e quindi $J_1^c J_2^c = (2)(2) = (4),\ (J_1 J_2)^c = ((1-i)^2)^c = (2)^c = (2)$.

Infine, si può vedere come interagiscono estensione e contrazione con radicale e radicale di Jacobson. Fissato $f : A \to B$ omomorfismo di anelli:

1. $f(\mathcal{N}(A)) \subseteq \mathcal{N}(B),\ f(\sqrt{I}) \subseteq \sqrt{f(I)}$ (dunque $(\sqrt{I})^e \subseteq \sqrt{I^e}$);
2. $\sqrt{J^c} = (\sqrt{J})^c$;
3. se f è surgettivo e $\ker(f) \subseteq I$, $(\sqrt{I})^e = \sqrt{I^e}$;
4. se f è surgettivo, $f(J(A)) \subseteq J(B)$;
5. se A è semilocale e f è surgettivo allora $f(J(A)) = J(B)$.

Mostriamo la 5, assumendo le precedenti. Siano $\{m_1, ..., m_r\}$ gli ideali massimali di A. In particolare m_i, m_j sono comassimali se $i \neq j$, dunque $J(A) = \bigcap_{i=1}^{r} m_i = \prod_{i=1}^{r} m_i \implies f(J(A)) = \prod_{i=1}^{r} f(m_i)$ (il prodotto commuta con l'estensione). Se $m_i \supseteq \ker(f),\ f(m_i)$ è massimale in B per la corrispondenza 1-1. Altrimenti $m_i^{ec} = m_i + \ker(f) = (1)$, cioè $f(m_i) = (1)$. Dunque

$f(J(A)) = \prod_{m_i \supseteq \ker(f)} f(m_i) = \bigcap_{m_i \supseteq \ker(f)} f(m_i)$ (gli $f(m_i)$ sono massimali e distinti per corrispondenza, e quindi comassimali), e un'intersezione di ideali massimali di B contiene $J(B)$. Si conclude poiché l'inclusione opposta viene dal punto 4.

Controesempio a 4: $i : \mathbb{Z}_{(p)} \hookrightarrow \mathbb{Q}$. $\mathbb{Z}_{(p)}$ è locale, ma non un campo, e i è iniettiva, quindi $i(J(\mathbb{Z}_{(p)})) \neq (0)$, ma $J(\mathbb{Q}) = (0)$.

Controesempio a 5: $\pi : \mathbb{Z} \to \mathbb{Z}/(4)$ è surgettiva, ma $\mathbb{Z}$ non è semilocale, e infatti $f(J(\mathbb{Z})) = f(0) = (0),\ J(\mathbb{Z}/(4)) = (\overline{2})$.

1.5 Fattorizzazione negli anelli

In questa sezione vogliamo studiare il problema della fattorizzazione negli anelli. Introdurremo un algoritmo per fattorizzare polinomi a coefficienti in un campo finito, e poi dimostreremo alcuni risultati classici su PID e UFD. Ci serve prima un altro risultato classico, il *teorema cinese del resto* (CRT):

Teorema 1.15 (Teorema cinese del resto)**.** Sia A un anello, e $I_1, ..., I_n$ ideali di A a due a due comassimali. Allora $\forall a_1, ..., a_n \in A\ \exists a \in A : a \equiv a_j \mod I_j$.

Dimostrazione. Usando il fatto che gli I_j sono a due a due comassimali, $\forall j \neq k\ \exists a_j^k \in I_j,\ a_k^j \in I_k : a_j^k + a_k^j = 1$. Sia $b_k = \prod_{j \neq k} a_j^k$. Osserviamo che $\forall j \neq k\ b_k \equiv 0 \mod I_j$ ($a_j^k \in I_j$) e $b_k \equiv 1 \mod I_k$, in quanto, $\forall j \neq k$, $1 = a_j^k + a_k^j \equiv a_j^k \mod I_k$. Quindi, se $a = \sum_{k=1}^{n} a_k b_k$, si ha $a \equiv a_j b_j \equiv a_j \mod I_j$. □

Corollario. Sia A un anello e $I_1, ..., I_n$ ideali di A. La mappa $f : A \to \prod_j A/I_j$, $f(a) = (a \mod I_j)_{j=1,...,n}$ (funzione prodotto delle proiezioni canoniche) è surgettiva se e solo se gli I_j sono a due a due comassimali. In tal caso, essendo $\ker(f) = \bigcap I_j = \prod I_j$, si ha che $A/\prod I_j \cong \prod A/I_j$.

Dimostrazione. Se gli I_j sono comassimali, vale il CRT e f è surgettiva. Viceversa, sfruttando la surgettività di f, $\forall j\ \exists a_j : f(a_j) = (0, ..., 1, ...0)$ (1 alla posizione j-esima). Allora $a_j \in I_k\ \forall k \neq j,\ 1 - a_j \in I_j$ (basta osservare che $f(1 - a_j) = (1, ..., 1) - (0, ..., 1, ..., 0) = (1, ..., 0, ...1)$, c'è uno 0 nella j-esima coordinata, quindi $1 - a_j \in I_j$), ovvero $1 = (1 - a_j) + a_j \in I_j + I_k$. □

Vediamo qualche applicazione del CRT. Sia A è un anello semilocale, con ideali massimali $m_1, ..., m_k$. Notiamo che due ideali massimali distinti sono comassimali, quindi per il CRT abbiamo $A/J(A) \cong \prod A/m_i$. In particolare, se $J(A) = 0,\ A$ è isomorfo a un prodotto diretto di campi. Ma in generale un anello semilocale non è prodotto diretto di locali: Se consideriamo l'anello $\mathbb{Z}_{(p,q)}$, l'insieme dei numeri razionali con denominatore coprimo con p e q, è semilocale, ma non locale (ha 2 ideali massimali, (p) e (q)), e non è un prodotto diretto di anelli locali, poiché è un dominio.

Un'altra applicazione classica è l'interpolazione di Lagrange: se $\alpha_1, ..., \alpha_n$ sono n elementi distinti di un campo K, e $\beta_1, ..., \beta n \in K$ (non necessariamente distinti), $\exists f \in K[x] : f(\alpha_i) = \beta_i \ \forall i$. Infatti, poiché gli $(x - \alpha_i)$ sono ideali massimali distinti, per il CRT è possibile risolvere il sistema di congruenze $f \equiv \beta_i \mod (x - \alpha_i)$. Cioè, $\forall i \ f(x) = p_i(x)(x - \alpha_i) + \beta_i \implies f(\alpha_i) = \beta_i$.

Ora vediamo un algoritmo per fattorizzare polinomi a coefficienti in $\mathbb{Z}/(p)$, noto come *algoritmo di Berlekamp*. Sia $f \in \mathbb{Z}/(p)[x]$ un polinomio a coefficienti in $\mathbb{Z}/(p)$ libero da quadrati (che, per il criterio della derivata, corrisponde alla condizione $\gcd(f, f') = 1$). Sia $B = \mathbb{Z}/(p)[x]/(f) : B$ è uno $\mathbb{Z}/(p)$-spazio vettoriale di dimensione $\deg(f)$. Sia $\varphi : B \to B, \ \varphi(b) = b^p$ l'omomorfismo di Frobenius. Allora $\ker(\varphi - id_B) \cong (\mathbb{Z}/(p))^n$ (come spazio vettoriale), dove n è il numero di fattori irriducibili di f. Inoltre, se $\overline{g} \in \ker(\varphi - id_B)$ e g è un rappresentante di $\overline{g}$ in B, allora $f = \prod_{a \in \mathbb{Z}/(p)} \gcd(f, g - a)$.

Dimostrazione. Per la prima parte, sia $f = \prod_{i=1}^{n} f_i$ la fattorizzazione in irriducibili di f. Poiché f è libero da quadrati, gli f_i sono tutti distinti, quindi, per il CRT, $B = \mathbb{Z}/(p)[x]/(\prod_{i=1}^{n} f_i) \cong \prod_{i=1}^{n} \mathbb{Z}/(p)[x]/(f_i)$, che è un prodotto di campi di caratteristica p. Se ora φ è l'omomorfismo di Frobenius, e $(b_1, ..., b_n) \in B$ (o, meglio, nell'immagine di B tramite l'isomorfismo del CRT), allora $(\varphi - id_B)(b_1, ..., b_n) = (b_1^p - b_1, ..., b_n^p - b_n)$. Se imponiamo che $(b_1, ...b_n)$ sia nel nucleo di $\varphi - id_B$, allora, $\forall i = 1, ..., n, \ b_i^p - b_i = 0$, equazione che ha come soluzioni tutti e soli i polinomi costanti, cioè gli elementi di $\mathbb{Z}/(p)$: infatti, l'equazione ha al più p soluzioni, e tutte le costanti la risolvono per il piccolo teorema di Fermat. Quindi $\ker(\varphi - id_B) \cong (\mathbb{Z}/(p))^n$.

Per la seconda parte, sia $(b_1, ..., b_n) \in \ker(\varphi - id_B)$, e sia $g \in \mathbb{Z}/(p)[x]$ tale che $g \equiv b_i \mod f_i$ per ogni i. Da quanto detto sopra sappiamo che i b_i sono costanti, quindi $\forall a \in \mathbb{Z}/(p) \ f_i | g - a \iff b_i = a$. Si ha che $\gcd(f, g - a) = \prod_{i=1}^{n} \gcd(f_i, g - a) = \prod_{i: \ b_i = a} f_i$, e moltiplicando su tutti gli $a \in \mathbb{Z}/(p)$ si trova $f = \prod_{i=1}^{n} f_i = \prod_{a \in \mathbb{Z}/(p)} \gcd(f, g - a)$.

□

Richiamiamo alcune definizioni:

- $a \in A \setminus A^*$ si dice **irriducibile** se $a = bc \implies b \in A^* \vee c \in A^*$;
- $a \in A \setminus A^*$ è **primo** se $a | bc \implies a | b \vee a | c$ (o, in alternativa, se (a) è un ideale primo);
- $a, b \in A$ sono **associati** se $\exists u \in A^* : a = ub$.

Osservazione. In generale, un elemento irriducibile può non essere primo. Per esempio, in $\mathbb{Z}[\sqrt{-5}]$, $2 | 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, ma 2 non divide nessuno dei due fattori.

Lemma 1.16. Sia A un dominio.

1. Se $a \in A$ è primo, allora è irriducibile.
2. A è un UFD se e solo se ogni elemento ammette una fattorizzazione in irriducibili e ogni irriducibile è primo.
3. Se A è un PID, allora ogni irriducibile è primo.

Dimostrazione. 1. Sia $a = bc$. In particolare, $a|bc$, e poiché a è primo, divide b o c. Senza perdere in generalità, supponiamo $a|b$. Allora $b = ax$, dunque $a = bc = acx \implies a(1-cx) = 0$. Visto che A è un dominio e $a \neq 0$, $cx = 1$ e c è invertibile.

2. Se A è un UFD, ovviamente ogni elemento (diverso da 0) ha una fattorizzazione in irriducibili. Se a è irriducibile e $a|bc$, allora $ad = bc$ per qualche d. Poiché a è irriducibile e c'è fattorizzazione unica, a deve comparire anche nella fattorizzazione in irriducibili di bc, dunque compare o in quella di b o in quella di c, ovvero $a|b$ o $a|c$. Viceversa, supponiamo che ogni elemento abbia una fattorizzazione e gli irriducibili sono primi, e mostriamo che la fattorizzazione è unica. Sia $x \in A$ tale che $x = \prod a_i = \prod b_j$, a_i, b_j irriducibili. Poiché b_1 è irriducibile, è primo, e in più divide x, che è il prodotto degli a_i, quindi deve dividere un certo a_i. Dunque si ha $a_i = b_1 c_1$, e per irriducibilità di a_i e b_1 c_1 è un'unità (ricordiamo che gli irriducibili non sono invertibili), ossia che a_i e b_1 sono associati. Quindi possono essere semplificati dalle rispettive fattorizzazioni, a meno di moltiplicare per unità. Possiamo ripetere il procedimento fino a esaurire i b_j, e a tal punto anche gli a_i saranno stati semplificati tutti, altrimenti si avrebbe che un'unità è un prodotto (non vuoto) di irriducibili, assurdo. Quindi le due fattorizzazioni dovevano essere la stessa.

3. Sia $a \in A$ irriducibile, e supponiamo $a|bc$. Allora $\exists d \in A : ad = bc$. Essendo A un PID, $(a, b) = (\alpha)$ per qualche α, quindi $a = \alpha\beta$. Ma a è irriducibile, quindi o α è invertibile o β è invertibile. Se $\beta \in A^*$, a e α sono associati, cioè $(a, b) = (\alpha) = (a)$ e perciò $a|b$. Se $\alpha \in A^*$, allora $(a, b) = (1)$, quindi $1 = ax + by$ per certi $x, y \implies c = cax + cby$, e $a|c$ in quanto $a|bc$.

□

Teorema 1.17. Se A è un PID, allora è un UFD.

Dimostrazione. Dal lemma precedente sappiamo che A è un UFD se e solo se esistono le fattorizzazioni e gli irriducibili sono primi. Inoltre, abbiamo anche che nei PID gli irriducibili sono primi, quindi è sufficiente mostrare che ogni elemento non nullo ammette una fattorizzazione. Innanzitutto, mostriamo che ogni catena ascendente di ideali in A è stazionaria. Sia $(a_0) \subseteq (a_1) \subseteq ...$ una catena ascendente di ideali di A. L'unione di tutti questi ideali in catena è un ideale, quindi è generato da un certo a. Poiché a è nell'unione degli ideali della catena, $a \in (a_k)$ per qualche k e dunque $(a) \subseteq (a_k)$. D'altra parte $(a_k) \subseteq (a)$,

quindi i due ideali sono uguali e la catena deve stabilizzarsi. Ora supponiamo per assurdo che $a_0 \in A$ non ammetta una fattorizzazione in irriducibili. In particolare non è irriducibile, quindi si ha $a_0 = a_1 b_1$, con a_1, b_1 non invertibili e non entrambi irriducibili. Senza perdere in generalità supponiamo che a_1 non sia irriducibile, allora $a_1 = a_2 b_2,\ a_2, b_2 \notin A^*$ e non entrambi irriducibili. Iterando questo procedimento, si genera una successione $a_0, a_1, ...$ in A tale che $\forall n \in \mathbb{N}\ a_{n+1} | a_n$ e a_n, a_{n+1} non sono associati, e dunque si ottiene una catena di ideali $(a_0) \subsetneq (a_1) \subsetneq ...$ infinita, ma non stazionaria, che è una contraddizione.

□

Osservazione. La proprietà che ogni catena ascendente di ideali di un anello è stazionaria caratterizza una classe molto importante di anelli, detti *noetheriani*, che ritorneranno più avanti.

1.6 Esercizi

1) Sia A un anello. $\exists f : A \to \prod_{i=1}^{k} A_i$ isomorfismo $\iff$ $\exists e_1, .., e_k \in A$ idempotenti (ovvero $e_i^2 = e_i\ \forall i$) ortogonali (cioè $e_i e_j = 0\ \forall i \neq j$) tali che $\sum_i e_i = 1$.

Soluzione. ($\implies$) Per $i = 1, ..., k$ sia $e_i = f^{-1}(0, ..., 1, ..., 0)$ (l'1 è nella posizione i-esima della k-upla) e mostriamo che e_i ha le proprietà volute. Notiamo che $f(e_i) = (0, ..., 1, ..., 0)$ è idempotente, quindi $f(e_i^2 - e_i) = f(e_i)^2 - f(e_i) = (0, ..., 0)$. Poiché f è iniettiva, $e_i^2 - e_i = 0$. Inoltre, se $i \neq j$, $f(e_i e_j) = f(e_i) f(e_j) = (0, ..., 0)$, visto che gli 1 sono in posizioni diverse. Infine $f(\sum_i e_i) = \sum_i f(e_i) = (1, ..., 1)$, che è l'identità del prodotto di anelli in arrivo e quindi immagine di $1 \in A$ (sfruttando ancora l'iniettività di f).

($\impliedby$) Sia $A_i = e_i A = \{e_i a \mid a \in A\}$. A_i è un anello con le operazioni indotte da A. Non è un sottoanello di A poiché non ha l'1, ma in A_i e_i $(= e_i \cdot 1)$ è l'identità: $e_i(e_i a) = e_i^2 a = e_i a$. Sia ora $f : A \to \prod_{i=1}^{k} A_i,\ f(a) = (e_1 a, ..., e_k a)$.

f è un omomorfismo: $f(a + b) = (e_1(a + b), ..., e_k(a + b)) = (e_1 a, ..., e_k a) + (e_1 b, ..., e_k b) = f(a) + f(b)$, $f(ab) = (e_1 ab, ..., e_k ab) = (e_1^2 ab, ..., e_k^2 ab) = (e_1 a \cdot e_1 b, ..., e_k a \cdot e_k b) = (e_1 a, ..., e_k a)(e_1 b, ...e_k b) = f(a) f(b)$,
$f(1) = (e_1, ..., e_k)$ che è l'identità in arrivo.

f è iniettiva: se $a \in \ker(f)$, $f(a) = (e_1 a, ..., e_k a) = (0, ..., 0) \implies e_i a = 0\ \forall i \implies 0 = a \sum_i e_i = a$.

f è surgettiva: sia $(e_1 a_1, ..., e_k a_k) \in \prod_{i=1}^{k} A_i$, con $a_i \in A$; abbiamo che $a = \sum_i a_i e_i$ viene mandato in $(e_1 a_1, ..., e_k a_k)$. Infatti, $f(a_i e_i) = (e_1 e_i a_i, ..., e_k e_i a_i) = (0, ..., e_i a_i, ..., 0)$ (termine non-zero al posto i), dunque $f(\sum_i a_i e_i) = \sum_i f(a_i e_i) = (e_1 a_1, ..., e_k a_k)$.

I prossimi esercizi saranno applicazioni del lemma di Zorn, e sfrutteranno il fatto che "elementi massimali di famiglie di ideali tendono a essere ideali primi".

2) Sia A un anello, e I un suo ideale. L'insieme $\mathcal{V}(I) = \{\mathfrak{p} \in Spec(A) \mid \mathfrak{p} \supseteq I\}$ ha elementi minimali per inclusione. In particolare, se $I = (0),\ \mathcal{V}(0) = \mathrm{Spec}(A)$ ha elementi minimali.

Soluzione. Mostriamo il caso $I = (0)$, il caso generale si risolve in modo simile, o passando al quoziente A/I. Sia $\Sigma = \mathrm{Spec}(A)$ ordinato con le inclusioni "rovesciate", in modo tale che, applicando il lemma di Zorn, l'elemento massimale scelto sarà *minimale* per inclusione. Ovviamente $\mathrm{Spec}(A)$ è non vuoto, poiché esistono ideali massimali. Sia ora I_λ una catena (decrescente!) di ideali in $\mathrm{Spec}(A)$. Il maggiorante della catena in questo caso sarà l'intersezione degli I_λ, sia esso P. Sappiamo già che è un ideale, mostriamo che è in Σ, ovvero è primo. Chiaramente P è proprio in quanto sottoinsieme di ideali propri. Se per assurdo $\exists a, b \notin I : ab \in I,\ ab$ sarebbe in tutti gli I_λ, ma esisterebbero λ_1, λ_2 con $a \notin I_{\lambda_1},\ b \notin I_{\lambda_2}$. Poiché gli I_λ sono totalmente ordinati, senza perdita di generalità $I_{\lambda_1} \subseteq I_{\lambda_2}$, quindi $b \notin I_{\lambda_1}$, che contraddice la primalità di I_{λ_1}. P è dunque primo e il lemma di Zorn vale, garantendo l'esistenza di primi minimali.

Definiamo $\mathrm{Min}(I)$ come l'insieme dei primi minimali che contengono I, e $\mathrm{Min}(A) = \mathrm{Min}(0)$ come l'insieme dei primi minimali di A. Di conseguenza abbiamo che $\mathcal{N}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Min}(A)} \mathfrak{p}$ e, più in generale, $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}$, in quanto i primi che contengono i minimali non contribuiscono all'intersezione.

3) Sia A un anello. Allora $\mathcal{D}(A)$ è unione di ideali primi.

Soluzione. Sia $\Sigma = \{I \subseteq A \text{ ideale} \mid I \subseteq \mathcal{D}(A)\}$, con l'ordinamento usuale. Mostriamo innanzitutto che Σ ha elementi massimali. Σ è non vuoto poiché contiene (0). Inoltre, se I_λ è una catena in Σ, l'unione di questi ideali è ancora un ideale ed è contenuto in $\mathcal{D}(A)$, quindi si può applicare il lemma di Zorn. Sia P un elemento massimale di Σ, e mostriamo che P è un ideale primo. Ovviamente, P è proprio perché 1 non è un divisore di zero, quindi non può essere in P. Per assurdo, siano $a, b \notin P$ tali che $ab \in P$. Gli ideali $(P, a),\ (P, b)$ contengono strettamente P, dunque, per massimalità di P, $\exists \alpha \in (P, a),\ \beta \in (P, b)$ non divisori di zero. Si può scrivere $\alpha = p + ka,\ \beta = q + hb,\ p, q \in P,\ h, k \in A$. Allora $\alpha\beta = pq + phb + qka + abhk \in P$, ma $\alpha\beta$ non è un divisore di zero: altrimenti, esisterebbe $\gamma \neq 0 : \alpha\beta\gamma = 0$, ma siccome $\beta\gamma \neq 0,\ \alpha$ sarebbe un divisore di zero. Ma $P \in \Sigma$, quindi contiene solo divisori di zero, assurdo. Per concludere, basta mostrare che $\mathcal{D}(A) = \bigcup_{I \in \Sigma} I$: infatti, se si fa l'unione sugli elementi massimali di Σ, si ottiene nuovamente $\mathcal{D}(A)$, ma è stato appena dimostrato che tali elementi sono ideali primi. Un'inclusione è banale, per l'altra basta osservare che, se x è divisore di zero e $y \neq 0$ è tale che $xy = 0,\ x \in \mathrm{Ann}(y) \subseteq \mathcal{D}(A)$.

4) Sia A un anello tale che ogni ideale primo è principale; allora A è un PIR (*principal ideal ring*), ovvero tutti i suoi ideali sono principali.

Soluzione. Per assurdo, supponiamo che $\Sigma = \{I \subseteq A \text{ ideale non principale}\}$ sia non vuoto, e ordinato nel modo usuale. Se I_λ è una catena in Σ, $I = \bigcup_\lambda I_\lambda$ è ancora un ideale non principale: altrimenti, se $I = (a),\ a$ sarebbe un elemento di qualche I_λ, ma allora $I = (a) \subseteq I_\lambda \subseteq I \implies (a) = I_\lambda$, che contraddice il

fatto che I_λ non è principale. Quindi, per Zorn, Σ ha un elemento massimale I, che non è principale, dunque, per ipotesi, non è primo. Allora $\exists a, b \notin I : ab \in I$. Si deduce che $(I, a) \supsetneq I$ e quindi che $(I, a) = (c)$ per qualche c. Scriviamo $c = x + ay,\ x \in I,\ y \in A$. Consideriamo ora l'ideale $I : (c)$. Osserviamo che $b \in I : (c)$, in quanto $bc = bx + aby \in I$ $(ab \in I)$. Poiché $b \notin I,\ I : (c) \supsetneq I \implies I : (c) = (d)$ per qualche d. Ora mostriamo che $I = (cd)$. Un contenimento è ovvio: $d \in I : (c) \implies cd \in I$. Per il contenimento opposto, fissiamo $i \in I$. Allora $i = kc,\ k \in A$, quindi $k \in I : (c) \implies k = hd,\ h \in A \implies i = hcd$. Quindi I è principale, assurdo.

5) Sia k un campo, $R = k[x, y, z, t],\ I = (yt^2 + x^3z^2t^2, z^2 + yt^2, x^2t^2)$. Calcolare $\sqrt{I}$, scrivendolo come intersezione di ideali primi.

Soluzione. Iniziamo semplificando i generatori di I: $x^2t^2 \in I$, quindi anche $x^3z^2t^2 \in I \implies yt^2 \in I$. e allora anche $z^2 \in I$. Abbiamo un sistema di generatori più semplici per I: $I = (yt^2, z^2, x^2t^2)$. I generatori di I sono dei monomi: in questo caso si dice che I è *monomiale*. È facile calcolare il radicale di un ideale di questo tipo: basta prendere ciascun generatore e "togliere" gli esponenti, come si farebbe per gli ideali di $\mathbb{Z}$ (lo dimostreremo in seguito). Quindi $\sqrt{I} = (yt, z, xt)$. Useremo ora ripetutamente questa proprietà degli ideali monomiali (che dimostreremo più avanti): se I è monomiale e f, g sono monomi coprimi, allora $(I, fg) = (I, f) \cap (I, g)$. Si ha $(yt, z, xt) = (y, x, zt) \cap (t, x, zt) = (y, x, z) \cap (y, x, t) \cap (t, x) = (x, y, z) \cap (t, x)$: nella prima uguaglianza abbiamo preso $I = (z, xt),\ f = y,\ g = t$, nella seconda $I = (y, x),\ f = z,\ g = t$. Non sono possibili ulteriori semplificazioni, in quanto i due ideali rimasti sono primi (e quindi irriducibili). Abbiamo trovato la cosiddetta *decomposizione primaria* di $\sqrt{I}$.

Osservazione. L'uguaglianza $(I, fg) = (I, f) \cap (I, g)$ NON è vera in generale! È invece vera in qualche caso particolare: uno è quello illustrato sopra. Un secondo caso si applica ad anelli più generali: si deve avere $(I, f, g) = (1)$. Infatti, in $A/I,\ (\overline{f})$ e $(\overline{g})$ sono comassimali, quindi $(\overline{fg}) = (\overline{f}) \cap (\overline{g})$. Sollevando entrambi i membri a ideali di A si ha $(I, fg) = (I, f) \cap (I, g)$. Questa uguaglianza può valere in generale, ma bisogna prendere il radicale di entrambi i lati: infatti, $\sqrt{(I, fg)} = \sqrt{(I, f)(I, g)} = \sqrt{(I, f)} \cap \sqrt{(I, g)}$.

2 L'anello $K[x_1, ..., x_n]$

L'obiettivo di questo capitolo è studiare gli ideali degli anelli di polinomi in n variabili a coefficienti in un campo K. Prima di tutto, analizzeremo le proprietà degli ideali monomiali, che sono i più semplici, vedremo un algoritmo per dividere polinomi in più variabili (la divisione euclidea non funziona per più di una variabile). Poi introdurremo le basi di Gröbner per studiare ideali generali. Infine studieremo l'anello $K[x_1, ..., x_n]$ da un punto di vista "geometrico", arrivando a dimostrare il Nullstellensatz di Hilbert. Per convenienza notazionale, useremo $\mathbf{x}$ per indicare $(x_1, ..., x_n)$ (ovvero $\mathbf{x}$ è un vettore con n entrate in $\mathbb{N}$). Se $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{N}^n$, poniamo $\mathbf{x^a} = x_1^{a_1}...x_n^{a_n}$. Inoltre, per tutto il resto del capitolo, $A = K[x_1, ..., x_n]$.

2.1 Ideali monomiali

Definizione (Ideale monomiale)**.** Un ideale I di $K[x_1, ..., x_n]$ si dice **monomiale** se ammette un sistema di generatori costituito da monomi.

Al momento, supponiamo anche che questi ideali sono finitamente generati: a breve dimostreremo che in realtà tutti gli ideali monomiali sono finitamente generati (lemma di Dickson).

Definiamo $\text{Mon}(A) = \{\mathbf{x^a} \mid \mathbf{a} \in \mathbb{N}^n\}$ come l'insieme dei monomi di A. Notiamo che c'è una corrispondenza 1-1 tra $\text{Mon}(A)$ e $\mathbb{N}^n$:

$$\mathbf{a} = (a_1, ..., a_n) \longleftrightarrow \mathbf{x^a} = x_1^{a_1}...x_n^{a_n}$$

In più tale corrispondenza preserva le operazioni naturali di somma in $\mathbb{N}^n$ e di prodotto in $\text{Mon}(A)$: $\mathbf{x^{a+b}} = \mathbf{x^a x^b}$.

Un generico elemento f di A è della forma $\sum c_\mathbf{a} \mathbf{x^a}$, al variare di $a \in \mathbb{N}^n$. Gli $\mathbf{x^a}$ il cui coefficiente è non nullo sono detti *monomi* di f. Ovviamente i monomi di f devono essere un numero finito, cioè $c_\mathbf{a} \neq 0$ solo per un numero finito di $\mathbf{a}$.

Proposizione 2.1 (Caratterizzazione degli ideali monomiali)**.** Sia I un ideale di A. Allora I è monomiale se e solo se ha la seguente proprietà: $\forall f \in A$, $f \in I$ se e solo se tutti i monomi di f appartengono a I.

Dimostrazione. Supponiamo che $I = (\mathbf{x^b})_{\mathbf{b} \in B}$ sia monomiale, dove $B \subseteq \mathbb{N}^n$, e sia $f = \sum c_\mathbf{a} \mathbf{x^a} \in A$. Ovviamente, se tutti i monomi di f sono in I, anche $f \in I$. Se invece $f \in I$, vogliamo mostrare che tutti i suoi monomi sono in I. Abbiamo che $\sum c_\mathbf{a} \mathbf{x^a} = f = \sum\limits_{\mathbf{b} \in B} c_\mathbf{b}(\mathbf{x}) \mathbf{x^b}$ (come al solito, solo un numero finito di coefficienti è diverso da 0). Si ha che $f = \sum\limits_{\mathbf{b} \in B} c_\mathbf{b}(\mathbf{x}) \mathbf{x^b} = \sum\limits_{\mathbf{b} \in B} \sum\limits_{\mathbf{d}} (c_{\mathbf{b},\mathbf{d}} \mathbf{x^d}) \mathbf{x^b}$ (scrivendo i coefficienti polinomiali $c_\mathbf{b}(\mathbf{x})$ come somma dei loro monomi)
$\implies f = \sum\limits_{\mathbf{b},\mathbf{d}} c_{\mathbf{b},\mathbf{d}} \mathbf{x^{b+d}}$. Uguagliando i coefficienti, si ha che $\forall \mathbf{a} : c_\mathbf{a} \neq 0$ esistono $\mathbf{b} \in B$, $\mathbf{d} \in \mathbb{N}^n$ tali che $\mathbf{x^a} = \mathbf{x^{b+d}} = \mathbf{x^b x^d}$, che appartiene a I in quanto $\mathbf{x^b} \in I$.

Viceversa, supponiamo che I sia tale che $f \in I \iff$ tutti i monomi di f stanno in I. Supponiamo che $I = (f_h)_{h \in H}$. Gli f_h generano I, quindi vi appartengono. Per ipotesi tutti i monomi degli f_h sono in I. Se J è l'ideale generato dai monomi degli f_h, per quanto detto sopra, $J \subseteq I$. Inoltre ogni f_h è combinazione lineare dei suoi monomi, che sono elementi di J, quindi $I \subseteq J$. Poiché $I = J$ e J è monomiale, si ha la tesi.

□

Mostriamo ora che tutti gli ideali monomiali sono finitamente generati. Prima ci serve qualche definizione.

Definizione ($\mathcal{E}$-sottoinsieme)**.** $E \neq \emptyset$ è un **$\mathcal{E}$-sottoinsieme di** $\mathbb{N}^n$ se $\forall \mathbf{a} \in E$, $\mathbf{b} \in \mathbb{N}^n$ $\mathbf{a} + \mathbf{b} \in E$.

Un $\mathcal{E}$-sottoinsieme E corrisponde all'ideale $I = (\mathbf{x}^{\mathbf{a}} \mid \mathbf{a} \in E)$.

Definizione. Sia E un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$. $\emptyset \neq F \subseteq E$ è una **frontiera** di E se $\forall \mathbf{a} \in E$ $\exists \mathbf{b} \in F,\ \mathbf{c} \in \mathbb{N}^n : \mathbf{a} = \mathbf{b} + \mathbf{c}$ (o, equivalentemente, $\mathbf{a} - \mathbf{b} \in \mathbb{N}^n$).

Se E è un $\mathcal{E}$-sottoinsieme, I l'ideale corrispondente, e F una frontiera di E, allora $\{\mathbf{x}^{\mathbf{a}} \mid \mathbf{a} \in F\}$ è un sistema di generatori per I.

Lemma 2.2 (Dickson)**.** Ogni $\mathcal{E}$-sottoinsieme E di $\mathbb{N}^n$ ammette una frontiera finita, e quindi ogni ideale monomiale di $K[x_1, ..., x_n]$ è finitamente generato.

Dimostrazione. Procediamo per induzione su n.

Passo base, $n = 1$: E è un sottoinsieme non vuoto di $\mathbb{N}$, quindi ha un minimo m. Chiaramente $\{m\}$ è una frontiera finita di E: se $l \in E$, $l - m \in \mathbb{N}$ in quanto $m \leq l$.

Passo induttivo, $n \implies n + 1$: sia $\pi : \mathbb{N}^{n+1} \to \mathbb{N}^n$, $\pi(a_0, a_1, ..., a_n) = (a_1, ..., a_n)$ (π "si dimentica" della 0-esima coordinata). Sia E un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^{n+1}$. Allora $\pi(E)$ è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$: infatti, è non vuoto e, se $\pi(\mathbf{a}) \in \pi(E)$, $\mathbf{b} \in \mathbb{N}^n$, $\pi(\mathbf{a}) + \mathbf{b} = \pi(\mathbf{a} + (0, \mathbf{b})) \in \pi(E)$. Per ipotesi induttiva, $\exists F' = \{\mathbf{a}_1, ...\mathbf{a}_k\} \subseteq E$ tale che $\pi(F')$ è una frontiera finita di $\pi(E)$. Ciascun $\mathbf{a}_i$ ha coordinate $(a_i^{(0)}, ..., a_i^{(n)})$. Sia $\overline{a} = \max\{a_i^{(0)} \mid 1 \leq i \leq k\}$, e $\forall\ 0 \leq a < \overline{a}$ sia $E_a = E \cap (\{a\} \times \mathbb{N}^n)$ l'insieme degli elementi di E con 0-esima coordinata a. Fissiamo $0 \leq a < \overline{a}$. Se $E_a = \emptyset$, poniamo $F_a = \emptyset$. Altrimenti, $\pi(E_a)$ è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$: è non vuoto e, se $\pi(\mathbf{a}) \in \pi(E_a)$, $\mathbf{b} \in \mathbb{N}^n$, $\pi(\mathbf{a}) + \mathbf{b} = \pi(\mathbf{a} + (0, \mathbf{b}))$, e $\mathbf{a} + (0, \mathbf{b}) \in E_a$. Per ipotesi induttiva, $\exists \mathcal{F}_a$ frontiera finita di E_a. Poniamo $F_a = \{0\} \times \mathcal{F}_a$. Sia ora $F = F' \cup \bigcup_{a=0}^{\overline{a}-1} F_a$. F è un insieme finito, facciamo vedere che è una frontiera di E. Sia $\mathbf{a} \in E$, e sia a_0 la sua 0-esima coordinata. Distinguiamo due casi:

- se $a_0 < \overline{a}$, allora $\mathbf{a} \in E_{a_0}$, quindi $\exists \mathbf{b} \in F_{a_0} : \mathbf{a} - \mathbf{b} \in \mathbb{N}^{n+1}$: infatti, la 0-esima entrata di $\mathbf{a} - \mathbf{b}$ è a_0, e le altre sono non-negative perché $\mathcal{F}_{a_0}$ è frontiera di $\pi(E_{a_0})$;
- se $a_0 \geq \overline{a}$, $\exists\ 1 \leq i \leq k : \pi(\mathbf{a}) - \pi(\mathbf{a}_i) \in \mathbb{N}^n$, quindi $\mathbf{a} - \mathbf{a}_i \in \mathbb{N}^n$ in quanto la 0-esima entrata è $a_0 - a_i \geq \overline{a} - a_i \geq 0$.

□

Si può fare di meglio: facciamo vedere che ogni $\mathcal{E}$-sottoinsieme E di $\mathbb{N}^n$ ammette un'unica frontiera minimale, detta *escalier* (una frontiera minimale è una frontiera di E minimale per inclusione). Innanzitutto, le frontiere minimali esistono: partiamo da una frontiera finita F (che esiste per Dickson), e se ci sono $\mathbf{b}_1, \mathbf{b}_2 \in F$ tali che $\mathbf{b}_2 - \mathbf{b}_1 \in \mathbb{N}^n$ (diverso da $\mathbf{0}$), allora $\mathbf{b}_2$ è superfluo e può essere eliminato dalla frontiera. Iterando questo passaggio finché è possibile, il procedimento si fermerà perché F è finita, e a quel punto la frontiera rimasta sarà minimale, ossia senza elementi "superflui". Un *escalier* di un $\mathcal{E}$-sottoinsieme E corrisponde a un sistema di generatori minimale dell'ideale monomiale I associato a E.

Proposizione 2.3. Sia E è un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$.

1. Se F è una frontiera minimale di E, allora F è finita.
2. E ammette un'unica frontiera minimale.

Dimostrazione. 1. Per il lemma di Dickson, E ammette una frontiera finita F'. Mostriamo che $F \subseteq F'$, e quindi che F è finita. Sia $\mathbf{a} \in F \subseteq E$. Poiché F' è una frontiera, $\exists \mathbf{b} \in F',\ \mathbf{c} \in \mathbb{N}^n : \mathbf{a} = \mathbf{b} + \mathbf{c}$. Ora $\mathbf{b} \in E$, quindi, usando il fatto che F è una frontiera, $\exists \mathbf{a}_1 \in F,\ \mathbf{c}_1 \in \mathbb{N}^n : \mathbf{b} = \mathbf{a}_1 + \mathbf{c}_1$, ovvero $\mathbf{a} - \mathbf{a}_1 = \mathbf{c}_1 + \mathbf{c}$. Ma $\mathbf{c}_1 + \mathbf{c} \in \mathbb{N}^n$, e se fosse diverso da $\mathbf{0}$, $\mathbf{a}$ sarebbe superfluo e F non sarebbe minimale. Quindi $\mathbf{c}_1 + \mathbf{c} = \mathbf{0} \implies \mathbf{c}_1 = \mathbf{c} = \mathbf{0} \implies \mathbf{a} = \mathbf{b} \in F'$.

2. Siano $F = \{\mathbf{a}_1, ..., \mathbf{a}_s\},\ F' = \{\mathbf{b}_1, ..., \mathbf{b}_t\}$ due frontiere minimali per E. Per definizione di frontiera, si può scrivere $E = \bigcup_{i=1}^{s} \mathbf{a}_i + \mathbb{N}^n = \bigcup_{j=1}^{t} \mathbf{b}_j + \mathbb{N}^n$. Ogni $\mathbf{a}_i$ è un elemento di E, quindi $\exists j : \mathbf{a}_i \in \mathbf{b}_j + \mathbb{N}^n$. Dunque è ben definita la funzione $\eta : \{1, ..., s\} \to \{1, ..., t\},\ \eta(i) = \min\{1 \leq j \leq t \mid \mathbf{a}_i \in \mathbf{b}_j + \mathbb{N}^n\}$. Innanzitutto, notiamo che η è surgettiva: se, per assurdo, j non fosse nell'immagine di η, allora $\forall i \in \{1, ..., s\}\ \exists j' < j : \mathbf{a}_i \in \mathbf{b}_{j'} + \mathbb{N}^n$. Ma in tal caso, $\{\mathbf{b}_1, ..., \mathbf{b}_{j-1}\}$ è una frontiera di E: infatti, poiché F è una frontiera, $\forall \mathbf{c} \in E\ \exists i : \mathbf{c} - \mathbf{a}_i \in \mathbb{N}^n$, e per ipotesi $\exists j' < j : \mathbf{a}_i - \mathbf{b}_{j'} \in \mathbb{N}^n$. Quindi $\mathbf{c} - \mathbf{b}_{j'} = (\mathbf{c} - \mathbf{a}_i) + (\mathbf{a}_i - \mathbf{b}_{j'}) \in \mathbb{N}^n$. Questo contraddice il fatto che F' sia una frontiera minimale di E. Dunque η è surgettiva, e $s \geq t$. Analogamente, c'è una mappa surgettiva ϑ da $\{1, ..., t\}$ a $\{1, ..., s\}$ (definita allo stesso modo, ma ribaltando i ruoli degli $\mathbf{a}_i$ e dei $\mathbf{b}_j$). Dunque, in realtà si ha $s = t$. Mostriamo ora che $F = F'$: $\forall i \in \{1, ..., s\}\ \mathbf{a}_i - \mathbf{b}_{\eta(i)} \in \mathbb{N}^n$ e $\mathbf{b}_{\eta(i)} - \mathbf{a}_{\vartheta(\eta(i))} \in \mathbb{N}^n$, quindi $\mathbf{a}_i - \mathbf{a}_{\vartheta(\eta(i))} \in \mathbb{N}^n$. Essendo F minimale, si deve avere $\mathbf{a}_i = \mathbf{a}_{\vartheta(\eta(i))}$, e vale anche $\mathbf{a}_i = \mathbf{b}_{\eta(i)}$. In particolare, $F \subseteq F'$, e, per minimalità di F', si ha l'uguaglianza cercata.

□

La proposizione precedente implica che ogni ideale monomiale I ammette un unico sistema di generatori *minimale* (e finito), che indichiamo con $G(I)$, e che corrisponde all'unico *escalier* dell'$\mathcal{E}$-sottoinsieme associato a I.

Uno dei vantaggi degli ideali monomiali è che combinarli tra loro con le usuali operazioni risulta molto facile.

Proposizione 2.4. Siano $I = (m_1, ..., m_s)$, $J = (n_1, ..., n_t)$ due ideali monomiali, e $m, u \in \mathrm{Mon}(A)$.

1. $I + J = (m_1, ..., m_s, n_1, ..., n_t)$. In particolare, $I + J$ è monomiale.
2. (proprietà di decomposizione) Se m, u sono monomi coprimi, allora $(I, m) \cap (I, u) = (I, mu)$.
3. $I \cap J = (\mathrm{lcm}(m_i, n_j))_{i,j}$.
4. $I : m = (\frac{m_i}{\gcd(m_i, m)})_{i=1,...,s}$.
5. $\sqrt{I} = (\sqrt{m_1}, ..., \sqrt{m_s})$, dove $\sqrt{m} = \prod_{x_h | m} x_h$ è la parte libera da quadrati di m. (Concretamente, un sistema di generatori per $\sqrt{I}$ si ottiene prendendo ciascun generatore di I e "rimuovendo" gli esponenti).

Dimostrazione. Dimostriamo la 1, la 2 e la 5.

1. Ovvia (e valida per ideali generali in anelli qualsiasi).
2. ($\supseteq$) Basta notare che

$$I \subseteq (I, m),\ I \subseteq (I, u),\ mu \in (I, m),\ mu \in (I, u).$$

($\subseteq$) Premettiamo la seguente osservazione: se I, J sono monomiali, allora $I \cap J$ è monomiale. Sia $f \in I \cap J$ e sia m un monomio di f. Poiché I, J sono monomiali, $m \in I,\ m \in J \implies m \in I \cap J$. Per la caratterizzazione, $I \cap J$ è monomiale. Sia ora $f \in (I, m) \cap (I, u)$, che è monomiale per 1. e per l'osservazione. Allora $(I, m) \cap (I, u)$ contiene tutti i monomi di f, quindi possiamo supporre che f sia un monomio. Se $f \in I$, chiaramente $f \in (I, mu)$. Se $f \notin I$, allora $m|f,\ u|f \implies f = am = bu$. Poiché m, u sono coprimi, $m|b$, ovvero $b = cm$. Dunque $f = cmu$, cioè $mu|f$.

5. Sia $H = (\sqrt{m_1}, ..., \sqrt{m_s})$. Notiamo che $\forall i\ \sqrt{m_i}|m_i$, e quindi $I \subseteq H$, e $m_i|(\sqrt{m_i})^{k_i}$ (dove k_i è il massimo esponente che compare in m_i), che implica $H \subseteq \sqrt{I}$. Passando ai radicali, otteniamo $\sqrt{H} = \sqrt{I}$. Per concludere, mostriamo che H è radicale. Usando ripetutamente la proprietà di decomposizione e sfruttando il fatto che $\sqrt{m_i}$ è prodotto di variabili (con esponente 1), abbiamo che $(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_s}) = \bigcap_{x_{h_1} | m_1} (x_{h_1}, \sqrt{m_2}, ..., \sqrt{m_s})$. Possiamo iterare questa procedura fino a ottenere che H è un'intersezione finita di ideali generati da variabili, che sono ideali primi (il quoziente è ancora un anello di polinomi a coefficienti in K, che è un dominio), e in particolare radicali. Infine, un'intersezione finita di ideali radicali è ancora radicale: se I, J sono radicali, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = I \cap J$. Dunque H è radicale.

□

Per esempio, in $K[x,y,z,t]$, l'ideale $H = (xy, zt)$ è radicale: infatti, per decomposizione, $(xy, zt) = (xy, z) \cap (xy, t) = (x, z) \cap (y, z) \cap (x, t) \cap (y, t)$. H è intersezione di 4 ideali primi, quindi è radicale.

Un'altra proprietà degli ideali monomiali è che è facile determinare se sono primi, primari, irriducibili o radicali, semplicemente guardando come è fatto il sistema di generatori minimale $G(I)$.

Proposizione 2.5. Sia I un ideale monomiale, e sia $G(I)$ il suo sistema di generatori minimale.

1. I è primo se e solo se $G(I)$ è un insieme di variabili (ossia monomi di grado totale 1).

2. I è radicale se e solo se $G(I)$ è un insieme di monomi liberi da quadrati.

3. I è irriducibile se e solo se in $G(I)$ compaiono solo potenze pure di variabili (cioè gli elementi di $G(I)$ sono della forma $x_i^{a_i}$).

4. I è primario se e solo se per ogni variabile x_i che divide un monomio di $G(I)$, $x_i^k \in G(I)$ per qualche $k \in \mathbb{N}$.

Dimostrazione. 1. È chiaro che se $G(I)$ è costituito da variabili allora I è primo. Viceversa, sia $m \in G(I)$. Allora $x_h | m$ per qualche h, dunque $m = x_h u$. Notiamo che $u \notin I$ in quanto divide propriamente m, e per minimalità di $G(I)$ non ci sono divisori propri di m in I. Poiché I è primo, $x_h \in I$, e per minimalità di $G(I)$ $m = x_h$.

2. Abbiamo già dimostrato che se I è generato da monomi liberi da quadrati, I è radicale (si veda la dimostrazione precedente). Invece, se I è radicale e $m \in G(I)$, allora $\sqrt{m} \in \sqrt{I} = I$ e $\sqrt{m} | m$. Per minimalità $\sqrt{m} = m$, ovvero m è libero da quadrati.

3. ($\Longrightarrow$) Sia $I = (m_1, ..., m_s)$ irriducibile. Per assurdo, se (diciamo) m_1 non fosse potenza di una variabile, si potrebbe scrivere come $x_h^k u$, con x_h^k, u coprimi. Allora

$$I = (m_1, ..., m_s) = (x_h^k, m_2, ..., m_s) \cap (u, m_2, ..., m_s)$$

è una decomposizione non banale di I, che quindi non sarebbe irriducibile.

($\Longleftarrow$) A meno di riordinare le variabili, possiamo supporre che $G(I) = \{x_1^{a_1}, ..., x_r^{a_r}\}$, per qualche $r \leq n$. Poniamo inoltre

$$\mathbf{y} = \{x_1, ..., x_r\},\ \mathbf{z} = \{x_{r+1}, ..., x_n\}.$$

Dunque $A = K[\mathbf{z}][\mathbf{y}]$. Per assurdo, siano J, L due ideali tali che $I = J \cap L,\ J, L \supsetneq I$. Mostriamo che $\exists p \in K[\mathbf{z}] : p(\mathbf{z}) x_1^{a_1 - 1} \cdots x_r^{a_r - 1} \in I$. Se esistesse tale p, avremmo un assurdo in quanto nessun elemento di $G(I)$ divide $p(\mathbf{z}) x_1^{a_1 - 1} \cdots x_r^{a_r - 1}$. Siano $f \in J \setminus I,\ g \in L \setminus I$. Si può assumere che nessun monomio di f e di g stia in I (altrimenti si potrebbero

sottrarre tali termini e il risultato sarebbe ancora fuori da I). Sappiamo che f è della forma $\sum c_{\mathbf{a}}(\mathbf{z})\mathbf{y}^{\mathbf{a}}$, con $c_{\mathbf{a}}(\mathbf{z}) \in K[\mathbf{z}]$, $\mathbf{a} = (a_1, ..., a_r) \in \mathbb{N}^r$, dove $\mathbf{y}^{\mathbf{a}} = x_1^{a_1} \cdots x_r^{a_r}$. Sia $\mathbf{y}^{\mathbf{d}}$ il monomio di grado totale minimo di f, $\deg(\mathbf{y}^{\mathbf{d}}) = \sum d_i$. Poiché $\mathbf{y}^{\mathbf{d}} \notin I$, $d_i < a_i \ \forall i$. In più, se u è un altro monomio di f, $\exists i : \deg_{x_i}(u) > d_i$ ($\deg_{x_i}(u)$ denota il grado di x_i nel monomio u). Infatti, se $\forall i \ \deg_{x_i}(u) \leq d_i$, per la minimalità di $\deg(\mathbf{y}^{\mathbf{d}})$ avremmo $\mathbf{y}^{\mathbf{d}} = u$. Definiamo $\mathbf{b} = (b_1, ..., b_r)$, $b_i = a_i - d_i - 1$. b_i è non-negativo perché $d_i < a_i$. Osserviamo che $\mathbf{y}^{\mathbf{b}+\mathbf{d}} = x_1^{a_1-1} \cdots x_r^{a_r-1} \notin I$; inoltre, se u è un monomio di f diverso da $\mathbf{y}^{\mathbf{d}}$, allora $\mathbf{y}^{\mathbf{b}}u \in I$. Quindi $\mathbf{y}^{\mathbf{b}}(f - c_{\mathbf{d}}(\mathbf{z})\mathbf{y}^{\mathbf{d}}) \in I \subseteq J$, ma $c_{\mathbf{d}}(\mathbf{z})\mathbf{y}^{\mathbf{b}+\mathbf{d}} = c_{\mathbf{d}}(\mathbf{z})x_1^{a_1-1} \cdots x_r^{a_r-1} \notin I$. Si deduce che $\mathbf{y}^{\mathbf{b}}f - \mathbf{y}^{\mathbf{b}}(f - c_{\mathbf{d}}(\mathbf{z})\mathbf{y}^{\mathbf{d}}) = c_{\mathbf{d}}(\mathbf{z})x_1^{a_1-1} \cdots x_r^{a_r-1} \in J \setminus I$. Ripetendo il ragionamento con g al posto di f, si trovano $h_{\mathbf{e}}(\mathbf{z})$ e $\mathbf{q}$ tali che $h_{\mathbf{e}}(\mathbf{z})\mathbf{y}^{\mathbf{q}+\mathbf{e}} = h_{\mathbf{e}}(\mathbf{z})x_1^{a_1-1} \cdots x_r^{a_r-1} \in L \setminus I$. Sia ora $p(\mathbf{z}) = c_{\mathbf{d}}(\mathbf{z})h_{\mathbf{e}}(\mathbf{z})$. Allora $p(\mathbf{z})x_1^{a_1-1} \cdots x_r^{a_r-1} \in J \cap L = I$, che conclude la dimostrazione.

4. ($\implies$) Supponiamo I primario, e sia $m \in G(I)$, $x_h | m \implies m = x_h u$. Come prima, $u \notin I$, e dato che I è primario $x_h^k \in I$, dunque $x_h^r \in G(I)$ (r è la più piccola potenza di x_h che appartiene a I).

   ($\impliedby$) A meno di riordinare le variabili, supponiamo che in $G(I)$ compaiano tutte le variabili da x_1 a x_r, per qualche $r \leq n$. Per ipotesi, $\forall\ 1 \leq i \leq r \ \exists k_i : x_i^{k_i} \in G(I) \subseteq I$, dunque $\sqrt{I} = (x_1, ..., x_r)$. Sia

   $$\varphi : K[x_1, ..., x_n] \hookrightarrow K(x_{r+1}, ..., x_n)[x_1, ..., x_r]$$

   l'inclusione naturale, dove nell'anello di arrivo le variabili $x_{r+1}, ..., x_n$ sono invertibili. Prima di tutto, verifichiamo che $I^{ec} = I$: basta il contenimento $\subseteq$ (l'altro vale sempre). Se $m \in G(I)$, allora $(m)^e = (m)$, in quanto m non è invertibile nel codominio di φ. Poiché estensione e somme finite commutano,

   $$I^e = ((m_1) + ... + (m_s))^e = (m_1)^e + ... + (m_s)^e = (m_1, ..., m_s) = I,$$

   o, più precisamente, l'immagine di I in $K(x_{r+1}, ..., x_n)[x_1, ..., x_r]$. Visto che φ è iniettiva, $I^{ec} = \varphi^{-1}(I) = I$. Inoltre, abbiamo che

   $$\sqrt{I^e} = \sqrt{I} = (x_1, ..., x_r),$$

   che è massimale nell'anello in arrivo; infatti il quoziente è il campo $K(x_{r+1}, ..., x_n)$. Essendo $\sqrt{I^e}$ massimale, I^e è primario, dunque $I^{ec} = I$ è primario in $K[x_1, ..., x_n]$.

□

2.2 Basi di Gröbner

In questa sezione vogliamo studiare il problema di appartenenza di un polinomio in $K[x_1, ..., x_n]$ a un dato ideale (*membership test*), che è una generalizzazione della divisione euclidea per anelli di polinomi in più variabili, e introdurremo le basi di Gröbner per risolverlo. Ci serve una definizione preliminare:

Definizione (Ordinamento monomiale)**.** $<$ è un **ordinamento monomiale** su $\mathbb{N}^n$ se:

- è un ordinamento totale;
- è un buon ordinamento;
- $\forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n,\ \mathbf{a} > \mathbf{b} \implies \mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$.

Esempio. *1. Ordine lessicografico (lex):* $\boldsymbol{a} = (a_1, ..., a_n) > (b_1, ..., b_n) = \boldsymbol{b}$ *se e solo se la prima coordinata non nulla di* $\boldsymbol{a} - \boldsymbol{b}$ *è positiva.*

2. DegLex: $\boldsymbol{a} > \boldsymbol{b}$ *se e solo se* $|\boldsymbol{a}| > |\boldsymbol{b}|$ *o* $|\boldsymbol{a}| = |\boldsymbol{b}|$ *e* $\boldsymbol{a} > \boldsymbol{b}$ *in lex. Qui* $|\boldsymbol{a}| = \sum_{i=1}^{n} a_i$ *è il grado totale del monomio* $\boldsymbol{x^a}$*. Secondo l'ordine DegLex, è più grande chi ha grado maggiore, e a parità di grado chi è più grande nell'ordine lessicografico.*

3. DegRevLex: $\boldsymbol{a} > \boldsymbol{b}$ *se e solo se* $|\boldsymbol{a}| > |\boldsymbol{b}|$ *o* $|\boldsymbol{a}| = |\boldsymbol{b}|$ *e l'ultima coordinata non nulla di* $\boldsymbol{a} - \boldsymbol{b}$ *è negativa.*

Esempio. *Consideriamo l'insieme di monomi*

$$\{x^2y^3z, x^5z, xyz^4, x^2y^2z^2, xy^4z, x^2yz^3\}.$$

Ordiniamoli secondo l'ordine DegRevLex, dove $x > y > z$*. Notiamo che tutti i monomi hanno grado 6, quindi vanno confrontati in base all'ordine lessicografico inverso. L'ultima coordinata dei vettori associati corrisponde all'esponente della* z*: chi ha l'esponente della* z *più grande sarà minore. Dunque il minimo di questo insieme è* xyz^4*, seguito da* x^2yz^3 *e da* $x^2y^2z^2$*. Ci sono tre monomi dove compare solo* z*: a questo punto si controlla quale monomio ha l'esponente della* y *più alto, ottenendo l'ordinamento* $xy^4z < x^2y^3z < x^5z$*. Si ha dunque*

$$xyz^4 < x^2yz^3 < x^2y^2z^2 < xy^4z < x^2y^3z < x^5.$$

È facile mostrare che lex, DegLex e DegRevLex sono ordinamenti monomiali. Vediamo solo che sono buoni ordini, esibendo esplicitamente il minimo di un insieme. Sia $S \subseteq \mathbb{N}^n$ non vuoto. Per lex, sia α_1 il minimo delle prime coordinate degli elementi di $S = S_0$ (che esiste poiché $\mathbb{N}$ è bene ordinato), e sia
$S_1 = \{\mathbf{a} \in S \mid a_1 = \alpha_1\}$. Poi siano α_2 il minimo delle seconde coordinate degli elementi di S_1, e $S_2 = \{\mathbf{a} \in S_1 \mid a_2 = \alpha_2\}$. Iterando per tutte le altre coordinate si arriva al minimo di S.

Per DegLex, sia $d = \min\{|\mathbf{a}| \mid \mathbf{a} \in S\}$ e sia $S_0 = \{\mathbf{a} \in S \mid |\mathbf{a}| = d\}$. A questo punto si trova il minimo secondo lex tra gli elementi di S_0, come descritto sopra.

Per DegRevLex, siano d e S_0 come prima, β_n il massimo di tutte le ultime coordinate degli elementi di S_0 (che esiste in quanto S_0 è finito),
$T_n = \{\mathbf{a} \in S_0 \mid a_n = \beta_n\}$. Dopo poniamo β_{n-1} il massimo delle penultime coordinate degli elementi di T_n, e $T_{n-1} = \{\mathbf{a} \in T_n \mid a_{n-1} = \beta_{n-1}\}$. Si può continuare così per tutte le coordinate, fino a raggiungere il minimo di S.

Definizione. Sia $0 \neq f = \sum c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} \in A$, e sia $<$ un ordinamento monomiale fissato.

- Il **multigrado** di f è $\mathrm{Deg}(f) = \max\{\mathbf{a} \in \mathbb{N}^n \mid c_\mathbf{a} \neq 0\}$.
- Il **coefficiente di testa** di f è $\mathrm{lc}(f) = c_{\mathrm{Deg}(f)}$.
- Il **monomio di testa** di f è $\mathrm{lm}(f) = \mathbf{x}^{\mathrm{Deg}(f)}$.
- Il **termine di testa** (*leading term*) di f è $\mathrm{lt}(f)$=$\mathrm{lc}(f)\mathrm{lm}(f)$= $c_{\mathrm{Deg}(f)}\mathbf{x}^{\mathrm{Deg}(f)}$.

Se $f, g \in A$, vale che:

- $\mathrm{Deg}(fg) = \mathrm{Deg}(f)\mathrm{Deg}(g)$;
- $\mathrm{Deg}(f+g) \leq \max\{\mathrm{Deg}(f),\mathrm{Deg}(g)\}$.

La dimostrazione è analoga a quella nel caso univariato.

Sia $I = (f_1 = xz^2 + z^2, f_2 = xy - y, f_3 = yz + y),\ f = xyz^2 - y$. Fissiamo l'ordinamento DegLex con $x > y > z$. Vogliamo sapere se $f \in I$. (Questo è un esempio del *membership test*). L'idea è di sottrarre a ogni passo un multiplo di f_i da f in modo da ridurne il multigrado. Per esempio,

$$f - yf_1 = xyz^2 - y - y(xz^2 + z^2) = -yz^2 - y.$$

Se aggiungiamo zf_3 otteniamo $yz - y$, e togliendo f_3 si ha $-2y$, che non divide nessuno dei termini di testa degli f_i. Se invece, al primo passaggio, consideriamo $f - z^2 f_2$, abbiamo $yz^2 - y$: sottraendo zf_3 si ottiene $-yz - y$; sommando f_3 si arriva a 0. Quindi, con due sequenze diverse di passaggi, abbiamo ottenuto 0 in uno solo dei due casi (che è però sufficiente per assicurare che $f \in I$). Vorremmo sapere in quali casi il resto della "divisione" tra f e I è indipendente dalla sequenza di passaggi effettuati. Prima, però, descriviamo questo algoritmo in generale, e dimostriamo che termina.

Definizione. Siano $f, g \in A \setminus \{0\}$. f *si riduce* ad h modulo g (in un passo) se esiste un monomio $c_\mathbf{a}\mathbf{x}^\mathbf{a}$ di f tale che $c_\mathbf{a}\mathbf{x}^\mathbf{a} | \mathrm{lt}(\mathbf{g})$ e $h = f - \frac{c_\mathbf{a}\mathbf{x}^\mathbf{a}}{\mathrm{lt}(g)}g$. In simboli: $f \xrightarrow{g} h$. Se $\overline{f}$ non ha nessun monomio divisibile per $\mathrm{lt}(g)$, diciamo che $\overline{f}$ è *ridotto* rispetto a g, e si scrive $f \to_* \overline{f}$, oppure $\overline{f}^g$.

Descriviamo l'algoritmo di divisione. Fissiamo un ordinamento monomiale. Siano $f \in A,\ I = (f_1, ..., f_m)$ un ideale di A; vogliamo scrivere

$$f = u_1 f_1 + ... + u_m f_m + r,$$

dove r è ridotto rispetto agli f_i. Definiamo un polinomio ausiliario p, che inizialmente sarà uguale a f. A ogni passo, si danno due casi:

1. $\forall i\ \mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$: allora poniamo $r = \mathrm{lt}(p)$ (che è ridotto), e il polinomio ausiliario "aggiornato" sarà new $p = p - \mathrm{lt}(p)$;
2. $\exists i : \mathrm{lt}(f_i) \mid \mathrm{lt}(p)$: allora poniamo new $p = p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}f_i$, e aggiungiamo $\frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}$ al vecchio valore di u_i.

Ripetiamo i passaggi finché $p = 0$. Notiamo che, prima o poi, si deve avere $p = 0$. Infatti, a ogni passo dell'algoritmo, p perde il suo termine di testa, generando una catena discendente dei suoi multigradi a ogni passo. Poiché l'ordinamento fissato è buono, tale catena deve essere finita, e in un numero finito di passi si avrà $p = 0$.

Osservazione. Il primo passo dell'algoritmo di divisione determina dove compare il *leading term* di f. Specificamente, si ha $\mathrm{Deg}(f) = \max\{\mathrm{Deg}(u_i f_i) \mid u_i \neq 0\}$ se $r = 0$, o $\mathrm{Deg}(f) = \max\{\mathrm{Deg}(u_i f_i), \mathrm{Deg}(r) \mid u_i \neq 0\}$ se $r \neq 0$.

Sia $S = \{f_\alpha\}_{\alpha\in\Lambda}$ un sottoinsieme di A, e fissiamo un ordinamento monomiale. Si definisce il *leading term ideal* di S come $\mathrm{Lt}(S) = (\mathrm{lt}(f_\alpha))_{\alpha\in\Lambda}$. Ovviamente $\mathrm{Lt}(S)$ è un ideale monomiale (in particolare è finitamente generato, per Dickson).

Siamo finalmente pronti per definire le basi di Gröbner.

Definizione (Base di Gröbner)**.** $G = \{g_1, ..., g_s\} \subseteq I \setminus \{0\}$ è una **base di Gröbner** per I se $\mathrm{Lt}(I) = (\mathrm{lt}(g_1),...,\mathrm{lt}(g_s)) = \mathrm{Lt}(G)$, ovvero se il *leading term ideal* di I è generato dai termini di testa degli elementi della base di Gröbner.

Notiamo che, nell'esempio precedente, poiché $-2y \in I,\ y \in \mathrm{Lt}(I)$, ma non è termine di testa di nessuno degli f_i, quindi $\{f_1, f_2, f_3\}$ non è una base di Gröbner.

L'importanza delle basi di Gröbner è dovuta al seguente teorema:

Teorema 2.6. Sia I un ideale di A. I seguenti fatti sono equivalenti:

1. $G = \{g_1, ..., g_s\}$ è una base di Gröbner per I;
2. $f \in I \iff f \xrightarrow{G}_* 0$;
3. $f \in I \iff f = u_1 g_1 + ... + u_s g_s,\ u_i \in A$ tali che $\mathrm{Deg}(f)=\max\{\mathrm{Deg}(u_i g_i) \mid u_i \neq 0\}$.

Dimostrazione. ($1 \implies 2$) Chiaramente, se f si riduce a 0 modulo g, allora f è combinazione lineare degli elementi di G, che appartengono anche a I. Viceversa, sia $f = u_1 g_1 + ... + u_s g_s + r$, con r ridotto rispetto a G. Poiché $f \in I,\ r \in I$, dunque $\mathrm{lt}(r) \in \mathrm{Lt}(I) = (\mathrm{lt}(g_1),...,\mathrm{lt}(g_s))$, in quanto G è una base di Gröbner. Ora, se $r \neq 0$, $\mathrm{lt}(r)$ è un multiplo di qualche $\mathrm{lt}(g_i)$. Ma, essendo r ridotto, non è divisibile per nessuno degli $\mathrm{lt}(g_i)$, quindi $r = 0$.

($2 \implies 3$) L'implicazione verso sinistra è ovvia. Per l'altra, se $f \in I$, si riduce a 0 tramite G, quindi si può scrivere $f = u_1 g_1 + \cdots + u_s g_s$, e per l'osservazione precedente, unitamente al fatto che $r = 0$, $\mathrm{Deg}(f) = \max\{\mathrm{Deg}(u_i g_i) \mid u_i \neq 0\}$.

($3 \implies 1$) Vogliamo mostrare che $\mathrm{Lt}(I) = (\mathrm{lt}(g_1), ... \mathrm{lt}(g_s))$. L'inclusione $\supseteq$ è ovvia, vediamo l'altra. Sia $f \in I$. Per ipotesi $f = u_1 g_1 + ... + u_s g_s$ e $\mathrm{Deg}(f) = \mathrm{Deg}(u_i g_i)$ per qualche i. Dunque $\mathrm{lt}(f) = \mathrm{lt}(u_i g_i) = \mathrm{lt}(u_i)\mathrm{lt}(g_i)$, ossia $\mathrm{lt}(g_i)|\mathrm{lt}(f)$ e quindi $\mathrm{lt}(f) \in (\mathrm{lt}(g_1),...,\mathrm{lt}(g_s))$, come voluto.

□

Il punto 3 implica immediatamente che una base di Gröbner di I è automaticamente un sistema di generatori per I, ma abbiamo già visto che il viceversa

è falso. Inoltre, se G è base di Gröbner per I, allora per ogni f il resto della divisione di f per G è unico: infatti, se $f = u_1 g_1 + ... + u_s g_s + r,\ f - r \in I$, dunque il resto di $f - r$ è 0, cioè il resto di f è r. Vale anche che l'unicità del resto implica che G è una base di Gröbner, ma è complicato da dimostrare.

Un'altra importante conseguenza di questo teorema è che $K[x_1, ..., x_n]$ è un anello noetheriano, ossia tutti i suoi ideali sono finitamente generati. Infatti, se I è un ideale, $\mathrm{Lt}(I)$ è un ideale monomiale e quindi finitamente generato, supponiamo da $\mathrm{lt}(g_1)$,..., $\mathrm{lt}(g_k)$. Allora $\{g_1, ..., g_k\}$ è una base di Gröbner, e quindi genera I. Abbiamo quindi trovato un sistema di generatori finito per I. (Questo è un caso particolare del *teorema della base di Hilbert*, che dimostreremo in seguito).

Adesso vorremmo trovare un modo per calcolare una base di Gröbner, dato un ordinamento e un sistema di generatori di un ideale. Iniziamo dal seguente esempio. Sia $I = (f_1 = xy^2 + x, f_2 = x^2 y + y) \subseteq K[x, y]$, e fissiamo l'ordinamento lex con $x > y$. Allora $\mathrm{Lt}(f_1, f_2) = (x^2 y, xy^2)$. Notiamo però che $x^2 \in \mathrm{Lt}(I)$, dato che $x f_1 - y f_2 = x^2 - y^2 \in I$, ma $x^2 \notin \mathrm{Lt}(f_1, f_2)$, quindi $\{f_1, f_2\}$ non è una base di Gröbner.

Definizione (S-polinomio)**.** Siano $f, g \in A \setminus \{0\}$, e fissiamo un ordinamento monomiale. L'***S*-polinomio** di f e g è $S(f, g) = \frac{\mathbf{x^c}}{\mathrm{lt}(f)} f - \frac{\mathbf{x^c}}{\mathrm{lt}(g)} g$, dove $\mathbf{x^c} = \mathrm{lcm}(\mathbf{x}^{\mathrm{Deg}(f)}, \mathbf{x}^{\mathrm{Deg}(g)})$.

Nell'esempio precedente, l'ostruzione al fatto che $\{f_1, f_2\}$ fosse una base di Gröbner è che $S(f_1, f_2)$ non si riduce a 0 (infatti è già ridotto). In un certo senso questa è "l'unica" ostruzione: infatti, vale il seguente criterio (di Buchberger): $\{g_1, ..., g_s\}$ è una base di Gröbner per l'ideale $(g_1, ..., g_s)$ se e solo se $S(g_i, g_j)$ si riduce a 0 per ogni $i \neq j$.
(non dimostrato)

Ora vediamo un metodo per ottenere basi di Gröbner da un sistema di generatori di un ideale, noto come *algoritmo di Buchberger*. Fissiamo un ordinamento monomiale $<$, e sia $F = \{f_1, ..., f_s\}$ un insieme di polinomi. L'output dell'algoritmo sarà una base di Gröbner (rispetto a $<$) per l'ideale $(f_1, ..., f_s)$ contenente gli f_i. Inizialmente, poniamo $G = F,\ \Sigma = \{(g_i, g_j) \in G \times G \mid i \neq j\}$. A ogni passo, calcoliamo $p = S(g_i, g_j)$ per ogni $(g_i, g_j) \in \Sigma$ e vediamo se si riduce a 0. In caso affermativo, rimuoviamo tale coppia da Σ, altrimenti ampliamo la nostra futura base di Gröbner G aggiungendovi p. In realtà, potremmo aggiungere la versione ridotta di p. Continuiamo il processo finché Σ non è vuoto. Dobbiamo dimostrare due cose:

1. l'algoritmo termina;

2. alla fine dell'algoritmo, l'insieme G ottenuto è una base di Gröbner.

Per 1. osserviamo che, ogni volta che aggiungiamo un polinomio p a G, abbiamo che $\mathrm{Lt}(G) \subsetneq \mathrm{Lt}(G \cup \{p\})$: se così non fosse, $\mathrm{lt}(p)$ sarebbe divisibile per $\mathrm{lt}(g)$ per qualche $g \in G$, e quindi p non sarebbe ridotto. Se l'algoritmo non terminasse, avremmo una catena ascendente infinita di ideali non stazionaria, impossibile

in quanto A è noetheriano (questa condizione è effettivamente equivalente alla generazione finita di tutti gli ideali, come vedremo più avanti).
La 2 è ovvia: Σ diventa vuoto se e solo se tutti gli S-polinomi si riducono a 0, che per il criterio di Buchberger è equivalente ad avere una base di Gröbner.

Esempio. *Sia $I = (f_1 = x^2y + z, f_2 = xz + y)$, con l'ordinamento DegLex, $x > y > z$. Il primo passo è il calcolo (e la riduzione) di $S(f_1, f_2)$, che si riduce a $-xy^2+z^2$. Poniamo $f_3 = xy^2-z^2$ (normalizzando il termine di testa) e calcoliamo $S(f_1, f_3)$, che si riduce a 0. (ora stiamo riducendo rispetto a $\{f_1, f_2, f_3\}$). Si continua come nell'algoritmo descritto sopra: $S(f_2, f_3) \to_* y^3+z^3 := f_4$, e si trova che $S(f_i, f_4) \to_* 0$ per $i = 1, 2, 3$. Quindi $\{x^2y+z, xz+y, xy^2-z^2, y^3+z^3\}$ è una base di Gröbner per I.*

Vediamo un risultato che ci permetterà di risparmiare molti conti nel calcolo della basi di Gröbner:

Proposizione 2.7. Siano $f, g \in A \setminus \{0\}$ tali che $\mathrm{lt}(f)$, $\mathrm{lt}(g)$ sono coprimi. Allora $S(f, g)$ si riduce a 0 tramite f, g, che sono dunque una base di Gröbner. (Naturalmente il risultato si generalizza a insiemi finiti di polinomi con termini di testa a due a due coprimi).

Dimostrazione. Scriviamo $f = \mathrm{lt}(f) + f_1,\ g = \mathrm{lt}(g) + g_1$. Per ipotesi abbiamo che $S(f, g) = \mathrm{lt}(g)f-\mathrm{lt}(f)g = (g - g_1)f - (f - f_1)g = f_1g - g_1f$. Se $f_1 = 0$ (o $g_1 = 0$), g (o f) è un monomio e $S(f, g) = -g_1f$ (o f_1g), che è un polinomio con tutti i monomi che dividono f (o g), e quindi si riduce a 0 tramite f (o g). Supponiamo ora che f_1 e g_1 siano diversi da 0. Osserviamo che $\mathrm{lm}(f_1g) \neq \mathrm{lm}(g_1f)$: se fossero uguali, $\mathrm{lm}(f_1g) = \mathrm{lm}(f_1)\mathrm{lm}(g) = \mathrm{lm}(g_1f) = \mathrm{lm}(g_1)\mathrm{lm}(f)$. Poiché $\mathrm{lm}(f)$ e $\mathrm{lm}(g)$ sono coprimi, si deve avere che $\mathrm{lm}(f)|\mathrm{lm}(f_1)$, assurdo in quanto f_1 è la coda di f. Quindi i *leading term* di f_1g e g_1f non si cancellano, dunque $\mathrm{lt}(f_1g-g_1f) = \mathrm{lt}(f_1g)$ o $\mathrm{lt}(g_1f)$, ovvero l'S-polinomio è riducibile tramite g o f. Effettuata la riduzione, abbiamo una nuova combinazione lineare $pg-qf$, con $\mathrm{Deg}(p) < \mathrm{Deg}(f)$ e $\mathrm{Deg}(q) < \mathrm{Deg}(g)$. Come prima, i termini di testa di pg e qf non si possono cancellare, per coprimalità di $\mathrm{lt}(f)$ e $\mathrm{lt}(g)$. Possiamo iterare fino a che $S(f, g)$ si è ridotto a 0, e a ogni passo abbiamo sottratto solo multipli di f e g. Quindi $\{f, g\}$ è base di Gröbner per (f, g).

□

Le basi di Gröbner non sono uniche: se $I = (x, y) \subseteq K[x, y]$, con ordinamento lex, $x > y$, allora $\forall a \in K,\ h \in \mathbb{N}\ G_{a,h} = \{x + ay^h, y\}$ è una base di Gröbner per I: infatti, $\mathrm{Lt}(G_{a,h}) = (x, y) = \mathrm{Lt}(I)$. Però c'è un'unica base di Gröbner "canonica" per ogni ideale (una volta fissato l'ordinamento!).

Definizione (Base di Gröbner ridotta)**.** Sia I un ideale di A, e fissiamo un ordinamento monomiale. $G = \{g_1, ..., g_s\}$ è una **base di Gröbner ridotta** se:

1. $\forall i = 1, ..., s\ \mathrm{lc}(g_1) = 1$ (i g_i sono normalizzati);
2. $\forall i \neq j\ \mathrm{lt}(g_i) \nmid \mathrm{lt}(g_j)$, ovvero {lt($g_1$),..., lt($g_s$)} è un sistema di generatori minimale;

3. $\forall i = 1, ..., s$ g_i è ridotto rispetto a $G \setminus \{g_i\}$.

Se G soddisfa 1. e 2., allora è detta base di Gröbner *minimale*.

Mostriamo che ogni ideale ammette una base di Gröbner ridotta, costruendone una esplicitamente: normalizzando i g_i e buttando via quelli inutili (che corrispondono a generatori superflui di $\mathrm{Lt}(G)$), possiamo supporre che G sia minimale. Iniziamo riducendo g_1 rispetto a $G \setminus \{g_1\}$, ottenendo g_1'. Poniamo $G_1 = G \setminus \{g_1\} \cup \{g_1'\}$, poi riduciamo g_2 rispetto a $G_1 \setminus \{g_2\}$, dando g_2'. Sia $G_2 = G_1 \setminus \{g_2\} \cup \{g_2'\}$, e riduciamo g_3 rispetto a $G_2 \setminus \{g_3\}$, ottenendo g_3', e così via. Alla fine si avrà una base di Gröbner G' ridotta. Infatti, $\forall i = 1, ..., s$ $\mathrm{lt}(g_i')$ $= \mathrm{lt}(g_i)$, quindi G' è minimale e gli S-polinomi sono rimasti invariati, quindi si riducono a 0 e G' è base di Gröbner, e anche ridotta. Facciamo vedere l'unicità: siano $G = \{g_1, ..., g_s\}$, $G' = \{g_1', ..., g_t'\}$ due basi di Gröbner ridotte per I. In quanto G, G' sono minimali, $\mathrm{Lt}(G)$ e $\mathrm{Lt}(G')$ sono sistemi di generatori minimali per $\mathrm{Lt}(I)$, quindi sono uguali. A meno di permutare i g_i' supponiamo $\mathrm{lt}(g_i) = \mathrm{lt}(g_i')$ per ogni I. Se per assurdo $g_i - g_i' \neq 0$, allora ha un *leading term*, che è diverso da $\mathrm{lt}(g_i)$ ed è un monomio di g_i o di $g_i'.(...)$

Vediamo alcune applicazioni delle basi di Gröbner. Per esempio, se I è un ideale di $K[\mathbf{x}]$, vorremmo poter dire se f è un unità in $K[\mathbf{x}]/I$. Abbiamo che $f \in (K[\mathbf{x}]/I)^* \iff \exists g : fg \equiv 1 \mod I \iff fg = 1 + i,\ i \in I \iff (f, I) = (1)$. Dunque il problema si riduce a un *membership test* sull'ideale (f, I), che sappiamo risolvere algoritmicamente grazie alle basi di Gröbner.

Un altro problema è identificare di un rappresentante canonico in $K[\mathbf{x}]/I$. L'osservazione chiave è che, se G è una base di Gröbner per I (fissato un ordinamento), la mappa $K[\mathbf{x}] \to K[\mathbf{x}]/I,\ f \mapsto \overline{f}^G$ è K-lineare. Infatti, è ben definita in quanto il resto modulo una base di Gröbner è unico. Inoltre, se $a, b \in K,\ f, g \in K[\mathbf{x}]$, notiamo che $\overline{f}^G,\ \overline{g}^G$ sono ridotti, dunque anche $a\overline{f}^G,\ b\overline{g}^G$ sono ridotti (in quanto a, b sono scalari) e quindi $a\overline{f}^g + b\overline{g}^G$ è ridotto: tutti i suoi monomi sono monomi di $\overline{f}^G$ o di $\overline{g}^G$, che non erano divisibili per nessuno dei $\mathrm{lm}(g_i)$ per ogni $g_i \in G$. Si ha che $a\overline{f}^g + b\overline{g}^G$ è (l'unico!) resto di $af + bg$, ovvero $af + bg \mapsto a\overline{f}^g + b\overline{g}^G$, che è la condizione di linearità. In particolare, ogni elemento di $K[\mathbf{x}]/I$ si scrive come combinazione K-lineare di monomi ridotti, cioè monomi non appartenenti a $\mathrm{Lt}(G)$.

Possiamo studiare anche la struttura di K-spazio vettoriale di $K[\mathbf{x}]/I$. Nell'esempio precedente, con $I = (x^2y + z, xz + y)$, possiamo trovare una K-base di monomi per il quoziente: essa sarà costituita dai monomi che non appartengono a $\mathrm{Lt}(G) = (x^2y, xz, xy^2, y^3)$. Notiamo che nessuna potenza di z appartiene a $\mathrm{Lt}(G)$, dunque $K[\mathbf{x}]/I$ ha dimensione infinita. In generale, $K[\mathbf{x}]/I$ ha dimensione finita se e solo se $\mathrm{Lt}(G)$ contiene potenze pure di tutte le variabili: infatti, se $x_i^{a_i} \in \mathrm{Lt}(G)$ per ogni $i = 1, ..., n$, nella base possono comparire solo monomi di grado minore o uguale a $a_1 + ... + a_n - n$, che sono in numero finito. Invece, se $x_i \notin \sqrt{\mathrm{Lt}(G)}$, tutte le potenze di x_i sono K-linearmente indipendenti e la dimensione è infinita.

Osservazione. La base lineare di $K[\mathbf{x}]/I$ dipende dalla base di Gröbner, e quindi dall'ordinamento scelto. In realtà, persino i rappresentanti "canonici" di $K[\mathbf{x}]/I$

dipendono dalla base di Gröbner. Ma ovviamente $\dim_K(K[\mathbf{x}]/I)$ non dipende dall'ordinamento: è sempre lo stesso spazio vettoriale!

Le basi di Gröbner sono utili per risolvere sistemi di equazioni polinomiali. Consideriamo il sistema

$$\begin{cases} x+y=a \\ x^2+y^2=a^2 \\ x^3+y^3=a^3 \end{cases}$$

con $a \in \mathbb{C}$, e cerchiamo le sue soluzioni complesse. L'ideale

$$I = (x+y-a, x^2+y^2-a^2, x^3+y^3-a^3) \subseteq \mathbb{C}[x,y,a]$$

ha base di Gröbner $G = \{x+y-a, y^2-ay, a^5-a^3\}$ (rispetto a lex, $x > y > a$). Imponendo che ciascun elemento di G sia uguale a 0 troviamo le soluzioni. L'ordinamento lex è comodo per risolvere sistemi perché gli ultimi elementi della base di Gröbner hanno poche variabili: infatti, un termine in a non può essere di testa se non sono eliminate prima la x e la y. Questo metodo di risoluzione di sistemi è analogo al metodo di eliminazione gaussiana per sistemi lineari.

Definizione. Sia I un ideale di $K[x_1, ..., x_n]$, e r un intero tra 1 e n.
L'***r*-esimo ideale di eliminazione** di I è $I_r = I \cap K[x_{r+1}, ..., x_n]$, cioè gli elementi di I in cui compaiono solo le ultime $n-r$ variabili. Una definizione alternativa è la seguente: se $f : K[x_{r+1}, ..., x_n] \hookrightarrow K[x_1, ..., x_n]$ è l'inclusione naturale, I_r è la contrazione di I tramite f.

Le basi di Gröbner si comportano bene con gli ideali di eliminazione; infatti vale questa proposizione:

Proposizione 2.8. Sia G una base di Gröbner per I rispetto all'ordinamento lex, con $x_1 > x_2 > ... > x_n$. Allora $G_r = G \cap K[x_{r+1}, ..., x_n]$ è base di Gröbner per I_r.

Dimostrazione. Per definizione $G_r \subseteq I_r$, quindi $\mathrm{Lt}(G_r) \subseteq \mathrm{Lt}(I_r)$. Per il contenimento opposto, sia $f \in I_r$, vogliamo mostrare che $\mathrm{lm}(f) \in \mathrm{Lt}(G_r)$. Usando il fatto che G è una base di Gröbner, $\exists g \in G : \mathrm{lm}(g) | \mathrm{lm}(f)$. Dato che $f \in I_r$, in $\mathrm{lm}(f)$ possono apparire solo le variabili $x_{r+1}, ..., x_n$, quindi lo stesso deve valere per $\mathrm{lm}(g)$. Allora in g non possono comparire le variabili $x_1, ..., x_r$ (perché scavalcherebbero $\mathrm{lm}(g)$ nell'ordinamento fissato), ossia $g \in K[x_{r+1}, ..., x_n]$ e quindi $g \in G_r$.

□

Vediamo altre applicazioni degli ideali di eliminazione. Possiamo calcolare l'intersezione di due ideali I e J, infatti vale

$$I \cap J = (tI, (1-t)J) \cap K[\mathbf{x}], \qquad (*)$$

dove $(tI, (1-t)J)$ è un ideale di $K[t, \mathbf{x}]$. A essere più precisi, consideriamo l'*estensione* di I e J a $K[t, \mathbf{x}]$, che già sappiamo essere $I[t]$ (risp. $J[t]$).
Dimostriamo $(*)$: se $f \in I \cap J$, è già in $K[\mathbf{x}]$; inoltre, $f = tf + (1-t)f$. Il primo

addendo è in tI e il secondo in $(1-t)J$. Viceversa, se $f \in (tI,(1-t)J) \cap K[\mathbf{x}]$, si può scrivere $f = t\sum a_i t^i + (1-t)\sum b_i t^i$, con $a_i \in I$ e $b_i \in J$. Notiamo che f è costante in t, quindi possiamo valutarla in qualsiasi t e ottenere sempre f. Sostituendo $t=0$, otteniamo $f = b_0 \in J$. Valutando in $t=1$, si ha $f = \sum a_i \in I$, come voluto. Data una base di Gröbner G per $(tI,(1-t)J)$ rispetto a lex, $t > x_1 > ... > x_n$, per la proposizione precedente $G_0 = G \cap K[\mathbf{x}]$ è una base di Gröbner per $(tI,(1-t)J) \cap K[\mathbf{x}] = I \cap J$.

Possiamo persino ridurre la divisione di ideali a una serie di intersezioni: se $I, J = (g_1, ..., g_r)$ sono due ideali, allora abbiamo che $I : J = \bigcap_{i=1}^{r} I : (g_i)$:

$f \in I : J \iff fg_i \in I \ \forall i \iff f \in \bigcap_{i=1}^{r} I : (g_i)$. In più vale che

$$I : (g_i) = \frac{1}{g_i}(I \cap (g_i)).$$

Infatti, $f \in I : (g_i) \iff fg_i \in I \cap (g_i) \iff f \in \frac{1}{g_i}(I \cap (g_i))$. Osserviamo che l'insieme a destra dell'uguale ha senso, in quanto tutti gli elementi di $I \cap (g_i)$ possono essere divisi per g_i. Avendo un algoritmo per il calcolo dell'intersezione, possiamo anche calcolare la divisione.

Concludiamo con un test di appartenenza al radicale di I: se $f \in K[\mathbf{x}]$, allora $f \in \sqrt{I} \iff (I, 1-tf) = K[t, \mathbf{x}]$. (Di nuovo, si considera l'estensione di I, cioè $I[t]$). Se $f \in \sqrt{I},\ f^n \in I$ per qualche $n \in \mathbb{N}$, quindi $1 = t^n f^n + 1 - t^n f^n \in (I, 1-tf)$. (Ricordiamo che $1-u^n$ è multiplo di $1-u$).
Viceversa, scriviamo $1 = \sum_{i=0}^{n} a_i t^i + h(1-tf),\ a_i \in I,\ h \in K[t, \mathbf{x}]$. Valutando entrambi i membri in $t = \frac{1}{f}$ (vedendoli come polinomi in t a coefficienti nelle funzioni razionali in $x_1, ..., x_n$)[1] si ottiene $1 = \sum_{i=0}^{n} \frac{a_i}{f^i}$. Moltiplicando entrambi i membri per f^n otteniamo $f^n = \sum_{i=0}^{n} a_i f^{n-i} \in I$, cioè $f \in \sqrt{I}$.

2.3 Varietà algebriche affini

In questa sezione studieremo ancora l'anello $K[x_1, ..., x_n]$, ma da un punto di vista più "geometrico", associando a ogni ideale un sottoinsieme dello spazio affine K^n.

Definizione. Sia $F \subseteq K[x_1, ..., x_n]$ un insieme di polinomi. La **varietà algebrica affine** associata a F è l'insieme

$$\mathbb{V}(F) = \{\alpha \in K^n \mid f(\alpha) = 0 \ \forall f \in F\}.$$

Per brevità, nel seguito ci riferiremo alle varietà algebriche affini chiamandole *varietà*.

[1] f dovrebbe essere diverso da 0, ma in tal caso è ovvio che $f \in \sqrt{I}$.

La varietà associata a F è dunque l'insieme delle soluzioni di un sistema di equazioni polinomiali. Notiamo che, se α si annulla in tutti gli elementi di F, si annulla in una qualunque combinazione lineare finita di elementi di F, quindi $\mathbb{V}(F)$ è anche la varietà associata all'*ideale* (F). In particolare, ogni varietà di K^n è della forma $\mathbb{V}(I)$ per qualche ideale I.

Definizione. Sia V una varietà di K^n. L'**ideale di annullamento** di V (o **ideale associato** a V) è l'insieme

$$\mathbb{I}(V) = \{p \in K[x_1, ..., x_n] \mid p(\alpha) = 0 \ \forall \alpha \in V\}.$$

È facile verificare che $\mathbb{I}(V)$ è un ideale. Quindi $K[x_1, ..., x_n]/\mathbb{I}(V)$ è un anello, detto l'*anello delle coordinate* di V. Indichiamo con $\mathcal{I}$ l'insieme degli ideali di $K[x_1, ..., x_n]$, e con $\mathcal{V}$ l'insieme delle varietà di K^n. Abbiamo appena definito due funzioni,

$$\phi : \mathcal{I} \to \mathcal{V}, \ \phi(I) = \mathbb{V}(I), \ \psi : \mathcal{V} \to \mathcal{I}, \ \psi(V) = \mathbb{I}(V).$$

Vediamone alcune proprietà:

1. Se $I \subseteq J$ sono ideali, allora $\mathbb{V}(I) \supseteq \mathbb{V}(J)$;
2. $I \subseteq \mathbb{I}(\mathbb{V}(I))$;
3. Se $V \subseteq W$ sono varietà, allora $\mathbb{I}(V) \supseteq \mathbb{I}(W)$;
4. $\mathbb{V}(\mathbb{I}(V)) = V$;
5. $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$;
6. $\mathbb{V}(IJ) = \mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$;
7. $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$.

Dimostriamo 1, 2, 4, 7.

1. Se $\alpha \in \mathbb{V}(J)$, allora si annulla in tutti i polinomi di J, che contiene I, quindi si annulla anche in tutti i polinomi di I, ovvero $\alpha \in \mathbb{V}(I)$.

2. Se $f \in I$, per definizione di $\mathbb{V}$ ogni elemento di $\mathbb{V}(I)$ si annulla in f, dunque $f \in \mathbb{I}(\mathbb{V}(I))$.

4. Sappiamo che $V = \mathbb{V}(I)$ per qulalche ideale I. Per la 2, $I \subseteq \mathbb{I}(\mathbb{V}(I))$, e per la 1 $\mathbb{V}(I) \supseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(I)))$, cioè $V \supseteq \mathbb{V}(\mathbb{I}(V))$. Viceversa, sia $\alpha \in V$. Per definizione di $\mathbb{I}(V)$, α annulla tutti i polinomi di $\mathbb{I}(V)$, dunque $\alpha \in \mathbb{V}(\mathbb{I}(V))$.

7. Poiché $I \subseteq \sqrt{I}$, si ha immediatamente $\mathbb{V}(\sqrt{I}) \subseteq \mathbb{V}(I)$. Per l'inclusione opposta, sia $g \in \sqrt{I}$, cioè $g^k \in I$. Poiché $\alpha \in \mathbb{V}(I)$, $g^k(\alpha) = g(\alpha)^k = 0$, quindi $g(\alpha) = 0$ e $\alpha \in \mathbb{V}(\sqrt{I})$. Da queste proprietà si deduce immediatamente che ϕ non è iniettiva (associa la stessa varietà a I e al suo radicale), mentre ψ lo è, e ha proprio ϕ come inversa sinistra. Se vogliamo avere qualche speranza che ϕ e ψ siano inverse, è necessario restringersi agli ideali radicali.

Definizione. Una varietà V è **riducibile** se $V = V_1 \cup V_2$, con V_1, V_2 sottovarietà proprie di V. Se V non è riducibile, si dice **irriducibile**.

Proposizione 2.9. Una varietà V è irriducibile se e solo se l'ideale $\mathbb{I}(V)$ è primo.

Dimostrazione. ($\implies$) Supponiamo che V sia irriducibile, e siano f, g tali che $fg \in \mathbb{I}(V)$. Osserviamo che possiamo scrivere $V = V_1 \cup V_2$, con $V_1 = V \cap \mathbb{V}(f),\ V_2 = V \cap \mathbb{V}(g)$. Infatti, per le proprietà elencate sopra, $V_1 \cup V_2 = (V \cap \mathbb{V}(f)) \cup (V \cap \mathbb{V}(g)) = V \cap (\mathbb{V}(f) \cup \mathbb{V}(g)) = V \cap \mathbb{V}(fg)$. Questa intersezione è uguale a V se $V \subseteq \mathbb{V}(fg)$, che è vero in quanto $fg \in \mathbb{I}(V) \implies (fg) \subseteq \mathbb{I}(V)$, quindi $\mathbb{V}(fg) \supseteq \mathbb{V}(\mathbb{I}(V)) = V$. Ma V è irriducibile, perciò $V_1 = V \cap \mathbb{V}(f) = V$ o $V_2 = V \cap \mathbb{V}(g) = V \implies V \subseteq \mathbb{V}(f)$ o $V \subseteq \mathbb{V}(g) \implies \mathbb{I}(V) \supseteq \mathbb{I}(\mathbb{V}(f)) \ni f$ o $\mathbb{I}(V) \supseteq \mathbb{I}(\mathbb{V}(g)) \ni g$, come voluto.

($\impliedby$) V è una varietà della forma $\mathbb{V}(I)$, per qualche ideale I. Scriviamo $V = V_1 \cup V_2$, con $V_1 = \mathbb{V}(I_1),\ V_2 = \mathbb{V}(I_2)$. Quindi abbiamo che

$$\mathbb{V}(I) = V = V_1 \cup V_2 = \mathbb{V}(I_1) \cup \mathbb{V}(I_2) = \mathbb{V}(I_1 I_2).$$

Applicando $\mathbb{I}$ otteniamo $\mathbb{I}(V) = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\mathbb{V}(I_1 I_2)) \supseteq I_1 I_2$. Poiché, per ipotesi, $\mathbb{I}(V)$ è primo, allora contiene I_1 o I_2, dunque $V = \mathbb{V}(\mathbb{I}(V)) \subseteq \mathbb{V}(I_1) = V_1$ (o $\mathbb{V}(I_2) = V_2$). Ovviamente $V \supseteq V_1$ e $V \supseteq V_2$, quindi $V = V_1$ o $V = V_2$, che è la tesi.

□

ATTENZIONE: non è vero in generale che, se $I \subseteq K[x_1, ..., x_n]$ è un ideale primo, la varietà $\mathbb{V}(I)$ è irriducibile!

Esempio. *Sia $K = \mathbb{Z}/(2),\ A = K[x, y],\ I = (x + y)$. Osserviamo che I è primo ($A/I \cong K[x]$). La varietà $\mathbb{V}(I)$ è costituita dai due punti $(0, 0)$ e $(1, 1)$, e si decompone in $\{(0, 0)\} \cup \{(1, 1)\} = \mathbb{V}(x, y) \cup \mathbb{V}(x - 1, y - 1)$, quindi $\mathbb{V}(I)$ è riducibile.*

Proposizione 2.10. Ogni varietà in K^n è unione finita di varietà irriducibili.

Dimostrazione. Sia Σ la famiglia dei controesempi (cioè delle varietà che non sono unione finita di irriducibili), e supponiamo per assurdo che non sia vuota. Vogliamo estrarre un elemento di Σ minimale per inclusione. Σ corrisponde a una famiglia non vuota S di ideali di $K[x_1, ..., x_n]$, e un elemento minimale di Σ corrisponde a un elemento massimale di S. Poiché $K[x_1, ..., x_n]$ è noetheriano, esiste un tale elemento massimale, che corrisponde a un elemento W di Σ minimale per inclusione. Per definizione di Σ, W non è unione finita di irriducibili; in particolare non è essa stessa irriducibile, quindi esistono $W_1, W_2 \subsetneq W$ tali che $W_1 \cup W_2 = W$. Per minimalità di W, W_1 e W_2 sono unione finita di irriducibili, e quindi anche W deve essere unione finita di irriducibili, assurdo.

□

Si può anche dimostrare che ogni varietà ha un'unica scrittura minimale come unione finita di irriducibili (dove per minimale si intende che, se $V = \bigcup_{i=1}^{k} V_i$ e $V_i \subseteq V_j$, possiamo buttare via V_i senza cambiare l'unione, e quindi la scrittura precedente non era minimale).

Il prossimo obiettivo è di dimostrare il *teorema di estensione*, che, dato un ideale I, ci permette di sollevare un punto di una varietà associata al primo ideale di eliminazione di I a un punto di $\mathbb{V}(I)$. Dobbiamo prima sviluppare un po' di teoria dei risultanti. Il risultante di due polinomi f, g è utile per determinare se f e g sono coprimi o no.

Lemma 2.11. Sia A un UFD e siano $f, g \in A[x] \setminus \{0\}$. Allora $\gcd(f,g) \notin A$ se e solo se $\exists P, Q \in A[x] \setminus \{0\} : \deg P < \deg f,\ \deg Q < \deg g$ e $Pg + Qf = 0$.

Dimostrazione. ($\Longrightarrow$) Se $\gcd(f,g) = h,\ \deg h \geq 1$, allora $f = hf_1,\ g = hg_1$, dunque $g_1 f - f_1 g = 0$. Ponendo $Q = g_1,\ P = -f_1$ si ha la tesi.

($\Longleftarrow$) Per assurdo, sia $\gcd(f,g) = a \in A$. Se $Q(A)$ è il campo dei quozienti di A, allora $a \in Q(A)^*$ e possiamo applicare l'identità di Bézout in $Q(A)[x]$, scrivendo $\tilde{P}g + \tilde{Q}f = 1$. Moltiplicando per P si ottiene $P\tilde{P}g + P\tilde{Q}f = P$. Usando il fatto che $Pg = -Qf$, abbiamo che $-\tilde{P}Qf + P\tilde{Q}f = P$, cioè $f(P\tilde{Q} - \tilde{P}Q) = P$. Ma allora $f|P$, quindi $\deg P \geq \deg f$, assurdo.

□

Siano $f = a_0 + a_1 x + ... + a_m x^m,\ g = b_0 + b_1 x + ... + b_n x^n \in A[x],\ a_m, b_n \neq 0$. Vogliamo trovare $P, Q \in A[x]$ come nel lemma. Quindi cerchiamo $P = p_0 + p_1 x + ... + p_{m-1} x^{m-1},\ Q = q_0 + q_1 x + ... + q_{n-1} x^{n-1}$ tali che $Pg + Qf = 0$. Sicuramente $\deg(Pg + Qf) \leq m + n - 1$. Il coefficiente di x^{m+n-1} di $Pg + Qf$ è $a_m q_{n-1} + b_m p_{n-1}$, il coefficiente di x^{m+n-2} è $a_{m-1} q_{n-1} + a_m q_{n-2} + b_{m-1} p_{m-1} + b_m p_{m-2}$, e similmente si calcolano gli altri coefficienti. Se $(q_{n-1}, ..., q_0, p_{m-1}, ..., p_0)^T$ è il vettore dei coefficienti di P e Q, il problema si riduce a risolvere il sistema lineare

$$\begin{pmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\ a_{m-1} & a_m & 0 & \cdots & b_{n-1} & b_n & \cdots & 0 \\ a_{m-2} & a_{m-1} & a_m & \cdots & b_{m-2} & b_{m-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_0 & a_1 & \cdots & a_{n-1} & b_0 & b_1 & \cdots & b_{n-1} \\ \vdots & \vdots & & \ddots & \vdots & \vdots & & \\ 0 & \cdots & & a_0 & 0 & \cdots & & b_0 \end{pmatrix} \begin{pmatrix} q_{n-1} \\ \vdots \\ q_0 \\ p_{m-1} \\ \vdots \\ p_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

che ha soluzione non nulla se e solo se il determinante della matrice non si annulla.

Definizione. Siano $f, g \in A[x]$. La **matrice di Sylvester** di f e g è la trasposta della matrice definita sopra, e si indica con $\mathrm{Syl}(f,g)$. Il **risultante** di f e g è il determinante della matrice di Sylvester: $\mathrm{Ris}(f,g) = \det(\mathrm{Syl}(f,g))$.

Per il lemma precedente, $\gcd(f,g) \notin A$ se e solo se il sistema lineare associato alla matrice di Sylvester ha una soluzione non nulla, ovvero se il risultante è 0. Se f, g sono come sopra, la matrice di Sylvester è una matrice quadrata $(m+n) \times (m+n)$ costruita così: nella prima riga ci sono i coefficienti di f, a partire dall'entrata in alto a sinistra, nella seconda ci sono i coefficienti di f

spostati di un posto verso destra, e così via fino all'n-esima riga. Nelle ultime m righe si ripete lo stesso procedimento con i coefficienti di g. Le entrate restanti sono uguali a 0. Dunque

$$\mathrm{Syl}(f,g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_n & \cdots & b_1 & b_0 & & \vdots \\ \vdots & \ddots & \ddots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b_n & \cdots & b_1 & b_0 \end{pmatrix}$$

Esempio. *Sia $f = ax^2 + bx + c \in K[x],\ a \neq 0$, e troviamo per quali a, b, c f ha una radice doppia (supponiamo K perfetto). Dal criterio della derivata sappiamo che questo corrisponde alla condizione* $\gcd(f, f') = 0$. *$f' = 2ax + b$ ha grado 1, e f ha grado 2, quindi Syl(f, g) è una matrice 3×3, con $m = 2,\ n = 1$. La prima riga contiene i coefficienti di f, le ultime 2 righe hanno i coefficienti di f'. Dunque*

$$\mathrm{Syl}(f,g) = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix},$$

e il suo determinante è $\mathrm{Ris}(f,g) = -a(b^2 - 4ac)$, *che si annulla se e solo se $b^2 - 4ac = \Delta$ si annulla ($a \neq 0$), che è l'usuale condizione sul discriminante di un'equazione quadratica.*

Il risultante ha le seguenti proprietà, che sono ereditate da quelle del determinante:

1. $\mathrm{Ris}(f,g) \in A$;
2. $\mathrm{Ris}(g,f) = (-1)^{\deg f \deg g}\mathrm{Ris}(f,g)$;
3. $\mathrm{Ris}(af,g) = a^{\deg g}\mathrm{Ris}(f,g)$, $\mathrm{Ris}(f,bg) = (-1)^{\deg f}\mathrm{Ris}(f,g)$, dove $a, b \in A$.

Proposizione 2.12. Siano $f, g \in A[x] \setminus \{0\}$. Allora esistono $P, Q \in A[x]$ con $\deg P < \deg f,\ \deg Q < \deg g$, e $\mathrm{Ris}(f,g) = Pg + Qf$.

Dimostrazione. Per ogni $i = 1, ..., m+n$, sommiamo all'ultima colonna della matrice di Sylvester la colonna i-esima moltiplicata per x^{m+n-i}, operazione che non cambia il determinante; l'ultima colonna sarà $(x^{n-1}f, ..., f, x^{m-1}g, ..., g)^T$. Sviluppando il determinante lungo tale colonna e separando i contributi di f e di g si ha che il risultante è della forma $Qf + Pg$, con $\deg Q < n = \deg g$ (dato che nella nuova matrice compare al più $x^{n-1}f$) e similmente $\deg P < m = \deg f$. □

Lemma 2.13. Siano $f, g \in K[x_1, ..., x_n]$, $f = a_0 + a_1 x_n + ... + a_m x_n^m$, $g = b_0 + b_1 x_n + ... + b_l x_n^l$, con gli a_i e i b_j in $K[x_1, ..., x_{n-1}]$. Sia $\beta \in K^{n-1}$ tale che:

1. $a_m(\beta) \neq 0$ (ovvero $f(\beta, x_n)$ ha grado m in x_n);
2. $g(\beta, x_n) \neq 0$, con $l - r = \deg(g(\beta, x_n))$ (cioè $b_{l-r+1}(\beta) = ... = b_l(\beta) = 0,\ b_{l-r}(\beta) \neq 0$).

Allora $\mathrm{Ris}_{x_n}(f, g)(\beta) = a_m(\beta)^r \mathrm{Ris}_{x_n}(f(\beta, x_n), g(\beta, x_n))$. In altre parole, "il risultante valutato in β è il risultante dei polinomi valutati".

Dimostrazione. $(\mathrm{Ris}_{x_n}(f, g))(\beta)$ è il determinante della matrice

$$\begin{pmatrix} a_m(\beta) & \cdots & a_0(\beta) & 0 & \cdots \\ & \ddots & & \ddots & \\ 0 & \cdots & a_m(\beta) & \cdots & a_0(\beta) \\ b_l(\beta) & \cdots & b_0(\beta) & 0 & \cdots \\ & \ddots & & \ddots & \\ 0 & \cdots & b_l(\beta) & \cdots & b_0(\beta) \end{pmatrix}$$

Se $b_l(\beta) \neq 0$, allora $r = 0$ e notiamo che la matrice di sopra è proprio $\mathrm{Syl}_{x_n}(f(\beta, x_n), g(\beta, x_n))$, il cui determinante è, per definizione, $\mathrm{Ris}_{x_n}(f(\beta, x_n), g(\beta, x_n))$. La formula è dunque verificata in questo caso. Se $b_l(\beta) = 0$, sviluppando lungo la prima colonna si ha $(\mathrm{Ris}_{x_n}(f, g))(\beta) = a_m(\beta)$ per il determinante di una matrice simile alla precedente, ma che ha $b_{l-1}(\beta)$ nella prima colonna. Ripetendo r volte si ottiene $(\mathrm{Ris}_{x_n}(f, g))(\beta) = a_m(\beta)^r$ per il determinante di una matrice con $b_{l-r}(\beta) \neq 0$ nella sua prima colonna, che è proprio la matrice di Sylvester di f e g valutata in β, ovvero $(\mathrm{Ris}_{x_n}(f, g))(\beta) = a_m(\beta)^r \mathrm{Ris}_{x_n}(f(\beta, x_n), g(\beta, x_n))$, come voluto.

□

Possiamo finalmente dimostrare il teorema di estensione:

Teorema 2.14 (di estensione delle soluzioni)**.** Sia K un campo algebricamente chiuso, ovvero $K = \overline{K}$, sia $I = (f_1, ..., f_s)$ un ideale proprio di $K[x_1, ..., x_n]$, e indichiamo con $I_1 = I \cap K[x_2, ..., x_n]$ il primo ideale di eliminazione di I. Scriviamo $f_i = c_i(x_2, ..., x_n) x_1^{N_i} + f_i'$, con f_i' la coda di f_i (abbiamo isolato il termine di grado più alto in x_1). Sia $\beta \in \mathbb{V}(I_1) \subseteq K^{n-1}$. Se $\beta \notin \mathbb{V}(c_1, ..., c_s)$, allora $\exists \alpha \in K$ tale che $(\alpha, \beta) \in \mathbb{V}(I)$.

Dimostrazione. Poiché $\beta \notin \mathbb{V}(c_1, ..., c_s)$, $\exists i : c_i(\beta) \neq 0$. Allora $\deg_{x_1}(f_i) = N_i \neq 0$. Se così non fosse, f_i sarebbe costante in x_1, ossia $f_i = c_i(x_2, ..., x_n)$, quindi $f_i \in I \cap K[x_2, ..., x_n] = I_1$. Ma $\beta \in \mathbb{V}(I_1)$, quindi $c_i(\beta) = 0$, contraddizione. Consideriamo $\varphi : K[x_1, ..., x_n] \to K[x_1], \varphi(f) = f(x_1, \beta)$. φ è un omomorfismo surgettivo, perciò $I^e = \varphi(I) = (\tilde{g}(x_1))$, in quanto $K[x_1]$ è un PID. Sia $g \in K[x_1, ..., x_n] : \varphi(g) = g(x_1, \beta) = \tilde{g}(x_1)$. Allora è sufficiente mostrare che $g(x_1, \beta)$ non è costante. Infatti, in tal caso avrebbe una radice α, essendo

K algebricamente chiuso. Quindi $\tilde{g}(\alpha) = g(\alpha, \beta) = 0$. Dato $f \in I$, $\varphi(f) = f(x_1, \beta) \in (\tilde{g}) \implies f(x_1, \beta) = \tilde{g}(x_1)\tilde{h}(x_1) \implies f(\alpha, \beta) = 0$. Dunque (α, β) si annulla in tutti i polinomi di I, cioè sta in $\mathbb{V}(I)$. Osserviamo che $f_i, g \in I$, quindi $\mathrm{Ris}_{x_1}(f_i, g) \in I_1$. Ma $\beta \in \mathbb{V}(I_1)$, ovvero $(\mathrm{Ris}_{x_1}(f_i, g))(\beta) = 0$. Notiamo inoltre che $c_i(\beta) \neq 0$ e $g(x_1, \beta) \neq 0$ (se fosse 0, tutti gli α in K sarebbero radici di g e avremmo finito). Siamo nelle ipotesi del lemma precedente, che implica (usando la notazione di prima) $0{=}(\mathrm{Ris}_{x_1}(f_i, g))(\beta) = c_i(\beta)^r \mathrm{Ris}_{x_1}(f_i(x_1, \beta), g(x_1, \beta))$. Dunque deve essere $\mathrm{Ris}_{x_1}(f_i(x_1, \beta), g(x_1, \beta)) = 0$, cioè $\gcd(f_1, g)$ non è costante, e poiché $K = \overline{K}$, f_1 e g hanno una radice in comune. In particolare g ha una radice, e non può essere costante.

□

Osservazione. Un caso semplice in cui il teorema di estensione vale sicuramente è quando uno dei c_i è costante (non nullo): infatti, in tal caso $\mathbb{V}(c_1, ..., c_s) = \mathbb{V}(1) = \emptyset$.

Ora abbiamo quasi tutti gli ingredienti necessari per dimostrare il famoso teorema degli zeri di Hilbert (*Nullstellensatz*). Ci serve un ultimo lemma:

Lemma 2.15. Sia K un campo infinito, $f \in K[x_1, ..., x_n]$ un polinomio di grado totale $N \geq 1$. Allora esistono $d_2, ..., d_n \in K$, $d \in K^*$ tali che

$$\varphi : K[x_1, ..., x_n] \to K[y_1, ..., y_n],\ x_1 \mapsto y_1,\ x_i \mapsto y_i + d_i y_1,\ 2 \leq i \leq n,$$

esteso a un isomorfismo di anelli, manda $f(x_1, ..., x_n)$ in

$$\varphi(f) = dy_1^N + f'(y_1, ..., y_n),$$

con $\deg_{y_1}(f') < N$.

Dimostrazione. Scriviamo $f = f_N + ... + f_1 + f_0$, con f_i omogeneo[2] di grado i. Osserviamo che

$$\varphi(x_1^{a_1} ... x_n^{a_n}) = \varphi(x_1)^{a_1} ... \varphi(x_n)^{a_n} = y_1^{a_1}(y_2 + d_2 y_1)^{a_2} ... (y_n + d_n y_1)^{a_n}.$$

Inoltre $\varphi(f) = \varphi(f_N) + ... + \varphi(f_0)$, e $\varphi(f_m)$ ha grado m. Dunque il termine di grado più alto (N) in y_1 proviene da $\varphi(f_N) = f_N(y_1, y_2 + d_2 y_1, ..., y_n + d_n y_1) = y_1^N f_N(1, d_2, ..., d_n) + f'$, con $\deg(f') < N$. Per concludere basta mostrare che $d = f_N(1, d_2, ..., d_n) \neq 0$ per qualche scelta di $d_2, ..., d_n$. Questo è vero in quanto $f_N(x_1, ..., x_n) = x_1^N f_N(1, \frac{x_2}{x_1}, ..., \frac{x_n}{x_1}) \neq 0$ (poiché $\deg f = N$), ed essendo K infinito non può annullarsi per ogni $(d_2, ..., d_n)$.

□

Notiamo che il lemma si applica al teorema degli zeri, che richiede che K sia algebricamente chiuso, e in particolare infinito.

Teorema 2.16 (Nullstellensatz debole)**.** Sia I un ideale di $K[x_1, ..., x_n]$, con $K = \overline{K}$. Allora $\mathbb{V}(I) = \emptyset$ se e solo se $I = (1)$.

[2]Un polinomio $f \in R[x_1, ..., x_n]$ si dice *omogeneo* di grado m se è combinazione R-lineare di monomi di grado m, o, in alternativa, se vale $f(tx_1, ..., tx_n) = t^m f(x_1, ..., x_n)$.

Dimostrazione. Ovviamente $\mathbb{V}(1) = \emptyset$. Dimostriamo l'implicazione opposta per induzione su n.

Passo base, $n = 1$: $A = K[x]$ è un PID, quindi $I = (f)$ e $\mathbb{V}(I)$ è l'insieme delle radici di f, che è vuoto se e solo se f è costante e non nullo, essendo $K = \overline{K}$.

Passo induttivo, $n-1 \implies n$: Sia $I = (f_1, ..., f_s)$. Se $f_1 \in K^*, I = (1)$. Altrimenti, per il lemma precedente esiste φ tale che $\varphi(f_1) = dy_1^N + f'$, $\deg(f') < N$. φ è un isomorfismo, quindi $\varphi(I)$ è un ideale di $K[y_1, ..., y_n]$ che contiene $\varphi(f_1)$. Poiché $\mathbb{V}(I)$ è vuota, anche $\mathbb{V}(\varphi(I))$ è vuota, in quanto φ è un isomorfismo. Ma il coefficiente di grado massimo in y_1 di f_1 è una costante, d, quindi, per il teorema di estensione, si deve avere $\mathbb{V}(\varphi(I)_1) = \emptyset$ (altrimenti potremmo sollevare un punto di $\mathbb{V}(\varphi(I)_1)$ a un punto di $\mathbb{V}(\varphi(I))$). $\mathbb{V}(\varphi(I)_1)$ è una varietà in K^{n-1}, dunque per ipotesi induttiva si ha $\varphi(I)_1 = (1)$, e chiaramente anche $\varphi(I) = (1)$ e $I = (1)$.

□

Richiamiamo il *test di appartenenza al radicale*: dato $f \in K[x_1, ..., x_n]$ e I un ideale, $f \in \sqrt{I} \iff (I, 1 - tf) = (1) = K[t, x_1, ..., x_n]$.

Teorema 2.17 (Nullstellensatz forte)**.** Sia I un ideale di $K[x_1, ..., x_n]$, con $K = \overline{K}$. Allora $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

Dimostrazione. ($\supseteq$) Dalle proprietà di $\mathbb{I}$ e $\mathbb{V}$ abbiamo $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(\sqrt{I}) = \mathbb{I}(\mathbb{V}(I))$.

($\subseteq$) Sia $f \in \mathbb{I}(\mathbb{V}(I))$. Per mostrare che $f \in \sqrt{I}$, usiamo il test di appartenenza al radicale: dobbiamo dunque far vedere che $(I, 1 - tf) = (1) \subseteq K[t, x_1, ..., x_n]$. Per il Nullstellensatz debole, questo è equivalente a mostrare che $\mathbb{V}(I, 1-tf) = \emptyset$. Sia $\alpha \in K^{n+1}$, con $\alpha = (b, \beta),\ b \in K,\ \beta \in K^n$. Si danno due casi:

1. $\beta \in \mathbb{V}(I)$: poiché $f \in \mathbb{I}(\mathbb{V}(I)),\ f(\beta) = 0$, quindi $(1 - tf)(\alpha) = 1 - bf(\beta) = 1 \neq 0$.

2. $\beta \notin \mathbb{V}(I)$: allora $\exists g \in I : g(\beta) \neq 0$. I è contenuto in $(I, 1 - tf)$ e $g(\alpha) = g(\beta) \neq 0$ (g è costante in t).

In entrambi i casi α non appartiene a $\mathbb{V}(I, 1 - tf)$, che è quindi vuota.

□

Ovviamente il nome suggerisce che la forma forte del teorema degli zeri implica la forma debole: infatti, se $\mathbb{V}(I) = \emptyset$, $\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\emptyset) = (1)$, quindi $I = (1)$.

Vediamo alcune conseguenze del Nullstellensatz. Una delle più importanti è la corrispondenza biunivoca tra ideali radicali e varietà: infatti $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$, $\mathbb{V}(\mathbb{I}(V)) = V$ (la seconda è sempre valida), e in questo caso $\mathbb{I}$ e $\mathbb{V}$ sono una l'inversa dell'altra. Un'altra conseguenza è la corrispondenza tra punti di K^n e ideali massimali di $K[x_1, ..., x_n]$. Innanzitutto notiamo che $\{\alpha\}$ è una varietà con ideale di annullamento $(x_1 - a_1, ..., x_n - a_n)$, dove $\alpha = (a_1, ..., a_n)$: infatti α chiaramente annulla $x_i - a_i$ per ogni i, ma non l'intero anello, in quanto $\mathbb{V}(1) = \emptyset$. Poiché $(x_1 - a_1, ..., x_n - a_n)$ è massimale, deve essere l'ideale di annullamento

di $\{\alpha\}$, che indicheremo con $\mathfrak{m}_\alpha$. Inoltre nessun altro punto si annulla in tutti i generatori di $\mathfrak{m}_\alpha$, quindi la varietà associata è costituita dal solo α, che è dunque una varietà. Se aggiungiamo l'ipotesi che K sia algebricamente chiuso, allora tutti gli ideali massimali di $K[x_1, ..., x_n]$ sono della forma $(x_1 - a_1, ..., x_n - a_n)$. Infatti, se m è massimale, è proprio, quindi per il Nullstellensatz debole $\mathbb{V}(m) \neq \emptyset$. Sia $\alpha \in \mathbb{V}(m)$. Allora $\mathfrak{m}_\alpha = \mathbb{I}(\alpha) \supseteq \mathbb{I}(\mathbb{V}(m)) = \sqrt{m} = m$, dove abbiamo usato il Nullstellensatz forte. Per massimalità di m si ottiene $m = \mathfrak{m}_\alpha$.

Teorema 2.18. Sia I un ideale di $K[x_1, ..., x_n]$, con $K = \overline{K}$. Fissiamo un ordinamento monomiale $<$ e una base di Gröbner G. Allora sono fatti equivalenti:

1. $|\mathbb{V}(I)| < \infty$;
2. $\forall i = 1, ..., n \ \exists g_i \in G : \mathrm{lm}(g_i) = x_i^{c_i}$ per qualche $c_i \in \mathbb{N}$;
3. $\dim_K A/I < \infty$.

Dimostrazione. ($1 \implies 2$) Se $|\mathbb{V}(I)| = 0$, $I = (1)$, quindi $1 \in G$ e possiamo prendere $c_i = 0$ per ogni i. Se $\mathbb{V}(I) = \{\alpha_1, ..., \alpha_s\}$, $\alpha_j = (a_{j1}, ..., a_{jn})$, per ogni i sia $f_i(x_i) = \prod_{j=1}^{s} (x_i - a_{ji})$. Osserviamo che f_i è un polinomio nella sola variabile x_i. Per definizione f_i si annulla in ogni α_j, quindi $f_i \in \mathbb{I}(\mathbb{V}(I)) = \sqrt{I} \implies f_i^{d_i} \in I$. Il suo monomio di testa sarà allora $x_i^{sd_i} \in \mathrm{Lt}(I) = \mathrm{Lt}(G)$. Quindi $\exists g_i \in G : \mathrm{lm}(g_i) | x_i^{sd_i} \implies \mathrm{lm}(g_i) = x_i^{c_i}$ per qualche $c_i \leq sd_i$.

($2 \implies 3$) Già visto.

($3 \implies 1$) Sia $d = \dim_K A/I < \infty$. Allora per ogni i l'insieme $\{\overline{1}, \overline{x_i}, ..., \overline{x_i}^d\}$ è linearmente dipendente, cioè $b_0 + b_1\overline{x_i} + ... + b_d\overline{x_i}^d = 0$. Sollevando la relazione all'anello $K[x_1, ..., x_n]$ si ha $b_0 + b_1 x_i + ... + b_d x_i^d \in I \cap K[x_i]$. Se $\alpha = (a_1, ..., a_n) \in \mathbb{V}(I)$, a_i deve essere una radice di un polinomio di grado d per ogni i, quindi la varietà associata è finita (e ha al più d^n elementi).

□

Proposizione 2.19. Supponiamo che K sia un campo algebricamente chiuso e che I sia un ideale radicale di $A = K[x_1, ..., x_n]$ con $|\mathbb{V}(I)| < \infty$. Allora I è un ideale 0-dimensionale (cioè la dimensione di Krull di A/I è 0), A/I è somma diretta finita di campi e $\dim_K A/I = |\mathbb{V}(I)|$.

Dimostrazione. "I è un ideale 0-dimensionale" significa "tutti gli ideali primi di A/I sono massimali", che è equivalente a dire che tutti i primi di A contenenti I sono massimali. Sia $\mathbb{V}(I) = \{\alpha_1, ..., \alpha_s\}$. Per il Nullstellensatz e il fatto che I è radicale, $I = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\{\alpha_1, ..., \alpha_s\}) = \bigcap_{i=1}^{s} \mathbb{I}(\{\alpha_i\}) = \bigcap_{i=1}^{s} \mathfrak{m}_{\alpha_i}$. Sia P un primo di A contenente I. Poiché P contiene l'intersezione degli $\mathfrak{m}_{\alpha_i}$, deve contenere un qualche $\mathfrak{m}_{\alpha_i}$, che è massimale, dunque si deve avere l'uguaglianza e P è massimale. Inoltre, gli $\mathfrak{m}_{\alpha_i}$ sono comassimali, quindi per il teorema cinese del resto $A/I = A/\bigcap_{i=1}^{s} \mathfrak{m}_{\alpha_i} = A/\prod_{i=1}^{s} \mathfrak{m}_{\alpha_i} \cong \prod_{i=1}^{s} A/\mathfrak{m}_{\alpha_i} \cong K^s$. In particolare

A/I è isomorfo a K^s anche come K-spazio vettoriale, dunque ha dimensione $s = |\mathbb{V}(I)|$.

□

Osserviamo che se R è un anello noetheriano e I è un suo ideale, anche R/I è noetheriano, poiché (per esempio) ogni catena ascendente di ideali di R/I corrisponde a una catena ascendente di ideali di R e deve dunque stabilizzarsi. Sappiamo che $A = K[x_1, ..., x_n]$ è noetheriano, dunque, se I è radicale e $K = \overline{K}$, A/I è noetheriano di dimensione 0. Inoltre abbiamo dimostrato che è una somma diretta finita di campi, che sono anelli noetheriani locali 0-dimensionali. Mostreremo in seguito che questo fatto vale per tutti gli anelli noetheriani 0-dimensionali.[3] Un'ultima conseguenza del teorema degli zeri è che, se K è algebricamente chiuso, $\mathrm{Min}(I)$, l'insieme dei primi minimali che contengono I, è finito. Infatti, consideriamo la varietà associata $\mathbb{V}(I)$ e la sua decomposizione minimale (che è unica) in irriducibili, $\mathbb{V}(I) = \mathbb{V}(I_1) \cup ... \cup \mathbb{V}(I_r)$. Allora $\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(V_1) \cap ... \cap \mathbb{I}(V_r)$, dove $\mathbb{I}(V_j)$ è primo in quanto V_j è irriducibile, ma sappiamo anche che $\sqrt{I} = \bigcap_{p \in \mathrm{Min}(I)} p$, quindi $\mathrm{Min}(I)$ è esattamente l'insieme dei primi associati alle componenti irriducibili di $\mathbb{V}(I)$: questo perché un altro elemento di $\mathrm{Min}(I)$ corrisponderebbe a un'altra componente irriducibile di $\mathbb{V}(I)$, violando l'unicità della decomposizione.

ATTENZIONE: in generale, se $\mathfrak{p}$ è primo, $\mathbb{V}(\mathfrak{p})$ non è necessariamente irriducibile (abbiamo già visto un esempio). Ma se $K = \overline{K}$, per il Nullstellensatz $\mathfrak{p} = \sqrt{\mathfrak{p}} = \mathbb{I}(\mathbb{V}(\mathfrak{p}))$, quindi $\mathbb{V}(\mathfrak{p})$ è irriducibile.

[3] Noti anche come anelli *artiniani*.

3 Moduli

3.1 Prime definizioni e proprietà

Definizione (A-modulo)**.** Sia A un anello e M un gruppo abeliano. M è un **A-modulo** se $\exists \cdot : A \times M \to M$ (detto *prodotto per scalari*) tale che:

- $\forall a \in A,\ m_1, m_2 \in M\ a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$;
- $\forall a, b \in A,\ m \in M\ (a + b) \cdot m = a \cdot m + b \cdot m$;
- $\forall a, b \in A,\ m \in M\ a \cdot (b \cdot m) = (ab) \cdot m$;
- $\forall m \in M\ 1 \cdot m = m$.

Notazione: indichiamo con $+$ l'operazione in M come gruppo abeliano, e con 0 la sua identità rispetto a $+$.

Attenzione a non confondere il prodotto per scalari con il prodotto nell'anello: nell'espressione $a \cdot (b \cdot m) = (ab) \cdot m$, a sinistra bm indica l'azione di b sul modulo M, a destra ab è il prodotto nell'anello A.

Vediamo alcuni esempi di moduli:

- Se K è un campo, ogni spazio vettoriale V su K è un K-modulo: infatti la definizione di modulo ricalca quella di spazio vettoriale.
- Ogni anello A è un A-modulo, dove il prodotto per scalari è semplicemente la moltiplicazione nell'anello. Più in generale, ogni ideale di A è un A-modulo, con il prodotto per scalari che coincide con il prodotto nell'anello. Ciò si deve alla proprietà di assorbimento degli ideali.
- Sia $f : A \to B$ un omomorfismo di anelli. L'azione

  $$\cdot : A \times B \to B,\ (a, b) \mapsto f(a)b$$

  definisce una struttura di A-modulo su B (si verifica facilmente con le proprietà di f). Questa operazione è anche detta *restrizione tramite* f, in quanto stiamo restringendo l'anello degli scalari da B al suo sottoanello $f(A)$.
- Ogni gruppo abeliano ha automaticamente una struttura di $\mathbb{Z}$-modulo, dove $\pm nx = \pm \underbrace{(x + \cdots + x)}_{n \text{ volte}}$, con $n \in \mathbb{N}$.

Definizione (Sottomodulo)**.** Sia M un A-modulo. $N \subseteq M$ è un A-sottomodulo di M se è un sottogruppo di M chiuso rispetto al prodotto per scalari.

Esempi:

- $\{0\}$ è sottomodulo (banale) di qualsiasi modulo M.
- Gli ideali di un anello A sono sottomoduli dell'A-modulo A.

- Sia $f : A \to B$ un omomorfismo di anelli. Allora $f(A)$ con la restrizione degli scalari è un A-sottomodulo dell'A-modulo B. Infatti, $\forall a, c \in A$ $a \cdot f(c) = f(a)f(c) = f(ac) \in f(A)$.

- Se M è un A-modulo e I è un ideale di A,

$$IM = \{\sum a_j m_j \mid a_j \in I,\ m_j \in M\}$$

  è un sottomodulo di M (come sempre le somme che definiscono gli elementi di IM sono finite).

Proviamo ora a definire i quozienti di moduli. Se M è un A-modulo e N un suo sottomodulo, sappiamo che M/N è un gruppo abeliano ben definito. Definiamo $\cdot : A \times M/N \to M/N,\ (a, \overline{m}) \mapsto \overline{am}$. Questa mappa è ben definita in quanto, se m, m' rappresentano lo stesso elemento di M/N, $m - m' \in N$ e quindi $a(m - m') = am - am' \in N$ dato che N è un sottomodulo. Dunque anche am, am' rappresentano lo stesso elemento di M/N. È facile verificare che si ha effettivamente una struttura di A-modulo su M/N.

Esempio. *Sia M un A-modulo e I un ideale di A. Allora M/IM è un A-modulo. Notiamo però che $\forall i \in I,\ \overline{m} \in M/IM$ $i\overline{m} = \overline{im} = \overline{0}$. Quindi possiamo dotare M/IM di una struttura di A/I-modulo, con $\overline{a} \cdot \overline{m} = \overline{am}$. Tale struttura si può vedere anche come quella indotta per restrizione dalla proiezione $\pi : A \to A/I$.*

Definizione. Sia M un A-modulo e L, N sottomoduli di M. Allora definiamo $L : N = \{a \in A \mid aN \subseteq L\} \subseteq A$.

$L : N$ è un ideale di A : infatti, $0 \in L : N$ ed è chiuso per somma e prodotto esterno, poiché N è un sottomodulo. Il caso più interessante è quello in cui $L = 0$. $0 : N = \mathrm{Ann}_A(N)$ è detto l'**annullatore** di N in A. Similmente all'esempio appena visto, ogni A-modulo N ha una struttura di A/I-modulo per ogni ideale $I \subseteq \mathrm{Ann}(N)$.

Se $\{M_h \mid h \in H\}$ è una famiglia di A-moduli, $\bigcap_{h \in H} M_h$ è un A-modulo. Possiamo anche definire

$$\sum M_h = \{\sum m_h \mid m_h \in M_h\}$$

(le somme sono ovviamente finite), e anche questo è un A-modulo. Sia $m \in M$, M un A-modulo. L'A-sottomodulo generato da m è $Am = \langle m \rangle_A = \{am \mid a \in A\}$. In generale, se $\{m_h \mid h \in H\} \subseteq M$, l'$A$-sottomodulo generato dagli m_h è $\langle m_h \mid h \in H \rangle_A = \{\sum a_h m_h \mid a_h \in A\}$ (somme finite). Bisogna fare attenzione all'anello degli scalari sul quale generiamo il modulo. Per esempio, l'A-modulo generato dalla variabile x è l'insieme dei polinomi di grado 1 con termine noto nullo (o il polinomio 0). Ma l'$A[x]$-modulo generato da x è fatto da prodotti di x per polinomi in x, ovvero polinomi con termine noto nullo.

Definizione (Modulo finitamente generato)**.** Sia M un A-modulo. Se esistono $m_1, ..., m_n \in M$ tali che $M = \langle m_1, ..., m_n \rangle_A$, allora M è un A-modulo **finitamente generato** (f.g.).

Per esempio, $A[x]$ non è un A-modulo finitamente generato: qualsiasi insieme finito di generatori $m_1, ..., m_n$ permetterebbe di ottenere solo polinomi di grado al più pari al massimo dei gradi degli m_i. Ma $A[x]$ è f.g. come $A[x]$-modulo: un insieme di generatori è dato dal solo $\{1\}$. In generale, ogni anello A è un A-modulo f.g., generato dall'elemento 1.

Un esempio classico è il seguente: $\mathbb{Q}$ non è finitamente generato come $\mathbb{Z}$-modulo. Infatti, $\langle \frac{a_1}{b_1}, ..., \frac{a_n}{b_n} \rangle_{\mathbb{Z}}$ può contenere solo frazioni con denominatori che dividono il massimo comun divisore dei b_i.

Ovviamente è possibile definire gli omomorfismi di moduli. Se M, N sono due A-moduli, $f : M \to N$ è un omomorfismo di A-moduli se

- è un omomorfismo di gruppi abeliani: $\forall x, y \in M \ f(x + y) = f(x) + f(y)$;
- $\forall a \in A, \ x \in M \ f(ax) = af(x)$.

La definizione è del tutto analoga a quella di applicazione lineare tra spazi vettoriali: infatti, un omomorfismo di A-moduli si dice anche "mappa A-lineare".

Esempio. *Fissato $a \in A$, $f : A \longrightarrow A$, $b \mapsto ab$ è un omomorfismo di A-moduli (ciò è equivalente alle proprietà distributiva e associativa del prodotto nell'anello). f però non è un omomorfismo di anelli.*

Vediamo un esempio un po' più complicato. Consideriamo la valutazione in a, $\varphi : A[x] \to A$, $\varphi(f(x)) = f(a)$. Questo è un omomorfismo di A-moduli: $\varphi(bf(x)) = (bf)(a) = bf(a) = b\varphi(f(x))$. Però lo si può vedere anche come omomorfismo di $A[x]$-moduli. Innanzitutto, notiamo che, essendo φ un omomorfismo di anelli, esso induce una struttura di $A[x]$-modulo su A tramite restrizione di scalari: $f(x) \cdot b = f(a)b$. Inoltre, $\varphi(f(x)g(x)) = f(a)g(a) = f(x) \cdot \varphi(g(x))$. Dunque ogni elemento di A induce una struttura di $A[x]$-modulo su A.

ATTENZIONE! Consideriamo $\mathbb{Z}$ come $\mathbb{Z}[x]$-modulo. Come detto sopra, sappiamo che possiamo indurre questa struttura tramite la valutazione in $a \in \mathbb{Z}$. Di certo, $\mathbb{Z}[x]/(x)$ e $\mathbb{Z}$ sono isomorfi come gruppi abeliani (e persino come anelli), ma non necessariamente come $\mathbb{Z}[x]$-moduli: questo dipende dalla scelta di a. Se $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ come $\mathbb{Z}[x]$-moduli, allora $x \in \mathrm{Ann}_{\mathbb{Z}[x]}(\mathbb{Z})$, cioè $x \cdot n = an = 0$ per ogni $n \in \mathbb{Z}$. Dunque deve essere $a = 0$. Similmente, $\mathbb{Z}[x]/(x - 5) \cong \mathbb{Z}$ come gruppi abeliani, ma lo sono come $\mathbb{Z}[x]$-moduli solo se $a = 5$. Inoltre notiamo che $M_1 = \mathbb{Z}[x]/(x)$ e $M_2 = \mathbb{Z}[x]/(x - 5)$ sono entrambi isomorfi a $\mathbb{Z}$ come $\mathbb{Z}[x]$-moduli, ma NON sono isomorfi tra loro! Infatti l'annullatore di M_1 contiene x, ma non $x - 5$, e l'annullatore di M_2 contiene $x - 5$, ma non x. Questo ha senso in quanto nei due casi l'azione di $\mathbb{Z}[x]$ su $\mathbb{Z}$ era diversa.

È facile verificare che valgono gli usuali teoremi di omomorfismo, i cui enunciati sono del tutto analoghi a quelli per i gruppi e per gli anelli.

Se $M = \langle s \rangle_A$, $f : M \longrightarrow N$ è univocamente determinato dall'immagine di s: infatti, $f(as) = af(s)$. In particolare $f : A \longrightarrow M$ è determinato dall'immagine

di 1, che genera A come A-modulo. La mappa $f : A \longrightarrow As = \langle s \rangle_A,\ f(a) = as$ non è un isomorfismo di $A-$moduli: è surgettiva per definizione di As, ma $\ker f = \mathrm{Ann}(s)$. Per i soliti teoremi di isomorfismo si ha $As \cong A/\mathrm{Ann}(s)$. Come per gli omomorfismi di gruppi e di anelli, possiamo definire il nucleo e l'immagine nel modo consueto, e nucleo e immagine sono sottomoduli dei moduli in cui vivono. Se $f : M \longrightarrow N$ è un omomorfismo di A-moduli, possiamo definire un ulteriore oggetto che non era ben definito negli altri casi, il **conucleo**:
$\mathrm{coker}\, f = N/\operatorname{Im} f$. Il conucleo misura quanto è lontana f dall'essere surgettiva, così come il nucleo misura quanto è lontana f dall'essere iniettiva.

Un altro esempio interessante di modulo è l'insieme degli omomorfismi tra due A-moduli M, N, indicato con $\mathrm{Hom}_A(M, N)$. Dati $f, g \in \mathrm{Hom}_A(M, N),\ a \in A$, poniamo $(f+g)(m) = f(m)+g(m),\ (af)(m) = af(m)$. Si verifica facilmente che con queste operazioni $\mathrm{Hom}_A(M, N)$ è un A-modulo. Se $N = M$ si parla di *endomorfismi* di M, denotati con $\mathrm{End}_A(M)$.

Mostriamo che $\mathrm{Hom}_A(A, M) \cong M$. Ogni omomorfismo da A in M è determinato dall'immagine di 1; quindi $\lambda : M \longrightarrow \mathrm{Hom}_A(A, M),\ m \mapsto \varphi_m,\ \varphi_m(1) = m$ è surgettiva, ed è lineare: $\varphi_{am+bn}(1) = am + bn = a\varphi_m(1) + b\varphi_n(1)$. Infine, $m \in \ker\lambda \implies \varphi_m = 0 \implies m = 0$, quindi λ è un isomorfismo.

Un altro risultato utile è il seguente: $\mathrm{Hom}_A(A/I, A/J) \cong (J : I)/J$. Infatti, $\varphi : A/I \longrightarrow A/J$ è determinata dall'immagine di $\overline{1}$. Se $\varphi(\overline{1}) = \overline{a}$, si deve avere che $\varphi(\overline{i}) = \overline{ia} = \overline{0}$, cioè $ia \in J\ \forall i \in I$, cioè $a \in J : I$. C'è quindi una mappa surgettiva $\lambda : J : I \longrightarrow \mathrm{Hom}_A(A/I, A/J),\ a \mapsto \varphi_a,\ \varphi(\overline{1}) = \overline{a}$. Inoltre $a \in \ker\lambda \iff \varphi_a(\overline{1}) = \overline{a} = \overline{0} \iff a \in J$. Per il primo teorema di isomorfismo $\mathrm{Hom}_A(A/I, A/J) \cong (J : I)/J$.

3.2 Moduli liberi

Dall'algebra lineare sappiamo che ogni spazio vettoriale ammette una base, quindi ci chiediamo se lo stesso vale per i moduli.

Definizione. Sia M un A-modulo e S un sottoinsieme di M.

- S è un **sistema di generatori** di M se $M = \langle S \rangle_A$;
- M è **finitamente generato** se ammette un sistema di generatori S finito (se M è generato da un unico elemento, si dice *ciclico*);
- un sistema di generatori S è **minimale** se $\forall s \in S\ \langle S \setminus \{s\} \rangle_A \subsetneq M$;
- S è **libero** se è formato da elementi linearmente indipendenti (cioè ogni combinazione lineare nulla di elementi di S a coefficienti in A deve avere tutti i coefficienti nulli);
- un insieme libero S è **massimale** se $\forall m \notin S\ S \cup \{m\}$ non è libero.

Definizione (Modulo libero)**.** Sia M un A-modulo. M è un modulo **libero** se ammette un sistema di generatori libero S, che in tal caso è detta **base** di M.

Ogni modulo su un campo K è libero, dato che ogni spazio vettoriale ammette una base (la definizione di base che abbiamo dato per i moduli è la stessa che è data per spazi vettoriali). Altri esempi di moduli liberi sono quelli della forma A^n, che hanno una base della forma $\{e_i \mid i = 1, ..., n\}$, la solita "base canonica" di vettori con 1 all'entrata i-esima e 0 altrove. Non tutti i moduli, però, sono liberi. Per esempio, $\mathbb{Z}/(n)(n \neq 0)$ è ovviamente uno $\mathbb{Z}/(n)$-modulo libero, ma non è libero come $\mathbb{Z}$-modulo: infatti, qualsiasi $x \in \mathbb{Z}/(n)$ è tale che $nx = 0$, dunque non ci sono sottoinsiemi liberi.

Nel caso dei moduli liberi, però, vale ancora il risultato che ogni base ha la stessa cardinalità. Quindi possiamo definire il *rango* di un modulo libero M come la cardinalità di una qualunque base di M: esso si indica con $\operatorname{rank} M$.

Proposizione 3.1. Sia M un A-modulo libero. Allora tutte le sue basi hanno la stessa cardinalità.

Dimostrazione. Sappiamo dall'algebra lineare che questo risultato è vero se A è un campo. Siano S, S' basi di M, e sia $\mathfrak{m}$ un ideale massimale di A. Consideriamo il modulo $M/\mathfrak{m}M$: esso ha una struttura di $A/\mathfrak{m}$-modulo, ma $A/\mathfrak{m}$ è un campo, ovvero $M/\mathfrak{m}M$ è un $A/\mathfrak{m}$-spazio vettoriale. Ci basta mostrare che $\overline{S}, \overline{S'}$, le immagini di S, S' tramite la proiezione al quoziente, sono basi dello *spazio vettoriale* $M/\mathfrak{m}M$: in tal caso avrebbero la stessa cardinalità, e quindi anche $|S| = |S'|$, poiché, se due elementi di S (S') avessero la stessa immagine in $\overline{S}$ ($\overline{S'}$), $\overline{S}$ ($\overline{S'}$) non sarebbe un insieme linearmente indipendenti (conterrebbe lo stesso elemento più di una volta). Dunque è sufficiente mostrare che la proiezione $\overline{S}$ di una base S al quoziente è base del modulo quoziente $M/\mathfrak{m}M$.

- $\overline{S}$ genera $M/\mathfrak{m}M$: $\forall m \in M\ m = \sum a_i s_i,\ a_i \in A,\ s_i \in S$, quindi $\overline{m} = \overline{\sum a_i s_i} = \sum \overline{a_i} \cdot \overline{s_i}$, con gli $\overline{s_i}$ che appartengono a $\overline{S}$, come voluto.
- $\overline{S}$ è linearmente indipendente: supponiamo che $\overline{0} = \sum \overline{a_i} \cdot \overline{s_i} = \overline{\sum a_i s_i}$. Vogliamo mostrare che $\forall i\ \overline{a_i} = \overline{0}$. Si ha che $\sum a_i s_i \in \mathfrak{m}M$, cioè $\sum a_i s_i = \sum c_j m_j,\ c_j \in \mathfrak{m},\ m_j \in M$. Poiché S genera M, scriviamo $m_j = \sum d_{ij} s_i$; si ha allora $\sum c_j m_j = \sum_j c_j (\sum_i d_{ij} s_i) = \sum_{i,j} c_j d_{ij} s_i$. Osserviamo che tutti i coefficienti degli s_i in questa seconda scrittura sono in $\mathfrak{m}$, in quanto i c_j sono in $\mathfrak{m}$. Per semplificare la notazione, chiamiamo tali coefficienti $r_i \in \mathfrak{m}$. Abbiamo quindi $\sum a_i s_i = \sum r_i s_i \implies 0 = \sum (a_i - r_i) s_i$. Essendo S libero, $\forall i\ a_i - r_i = 0 \implies a_i = r_i \in \mathfrak{m}$. Dunque in $A/\mathfrak{m}$ $\overline{a_i} = \overline{0}$ per ogni i.

□

Sappiamo che per un K-spazio vettoriale V e $B, B' \subseteq V$ valgono le seguenti:

1. B è base di V se e solo se ogni elemento di V ha un'unica scrittura come combinazione lineare di elementi di B;
2. se B, B' sono sistemi di generatori minimali di V, hanno la stessa cardinalità;

3. se B è un insieme linearmente indipendente (o libero) massimale di V, allora è una base;

4. se B è un sistema di generatori minimale di V, allora è una base;

5. se V ha dimensione finita e W è un sottospazio di V, allora W ha dimensione finita;

6. ogni sottospazio W di V ammette una base.

Se M è un A-modulo libero e S una sua base, ci chiediamo se valgono risultati analoghi.

La 1 è vera: se $m = \sum a_i s_i = \sum b_i s_i,\ 0 = \sum (a_i - b_i)s_i$. Poiché S è una base, $\forall i\ a_i - b_i = 0 \implies a_i = b_i$.

Tutte le altre sono false. Vediamo dei controesempi:

2. Prendiamo $A = \mathbb{Z},\ M = \mathbb{Z},\ S_1 = \{1\},\ S_2 = \{2, 3\}$. 1 genera $\mathbb{Z}$, così come 2 e 3, in quanto $3 - 2 = 1$ e 1 genera $\mathbb{Z}$. Ma 2 o 3 non possono generare $\mathbb{Z}$ da soli. Quindi S_1, S_2 sono sistemi di generatori minimali con cardinalità differenti.

3. Prendiamo $A = \mathbb{Z},\ M = \mathbb{Z},\ S = \{2\}$. 2 è un elemento libero, ma $\{2, n\}$ non è libero per ogni $n \neq 2$, per la relazione $n \cdot 2 - 2 \cdot n = 0$, ovvero 2 è un insieme libero massimale, che però non genera $\mathbb{Z}$.

4. Prendiamo $A = \mathbb{Z},\ M = \mathbb{Z},\ S = \{2, 3\}$. S è un sistema di generatori minimale (visto in 2.), ma non è libero (visto in 3.).

5. Un controesempio si ottiene prendendo come A un anello non noetheriano (e.g. $K[x_1, x_2, ...]$), come M lo stesso A, che è generato dal solo 1, e come sottomodulo N di M un ideale di A non finitamente generato (e.g. $(x_1, x_2, ...)$).

6. Sia $A = \mathbb{Z}/(6),\ M = \mathbb{Z}/(6),\ N = (\overline{2})$: M è chiaramente un A-modulo libero, ma $(\overline{2})$ non lo è: infatti $\overline{3} \in \mathrm{Ann}(\overline{2})$, quindi non ci sono elementi linearmente indipendenti.

Definizione (Somma e prodotto diretto)**.** Sia $\{M_h\}_{h \in H}$ una famiglia di A-moduli. La **somma diretta** degli M_h, indicata con $\bigoplus_{h \in H} M_h$, è l'insieme delle stringhe $(m_h)_{h \in H}$ tali che al più un numero finito di m_h è diverso da 0.

Il **prodotto diretto** degli M_h, denotato da $\prod_{h \in H} M_h$, è, come insieme, il prodotto cartesiano degli M_h (come la somma diretta, ma senza la restrizione sul numero di elementi diversi da 0).

Sia la somma che il prodotto per scalari sono effettuate componente per componente.

Entrambi sono effettivamente degli A-moduli: le proprietà da verificare discendono dalla struttura di A-modulo degli M_h. Inoltre la somma diretta degli M_h è un sottomodulo del prodotto diretto degli M_h, e coincidono se H è un insieme finito.

Esempio. *Sia S un insieme. Definiamo $A^S = \bigoplus_{s \in S} A$. A^S è un modulo libero con base formata da $\{e_s \mid s \in S\}$. e_s ha zeri dappertutto tranne che un 1 alla posizione s.*

Se $M = \langle S \rangle_A$, possiamo definire una mappa $f : A^S \longrightarrow M,\ e_s \mapsto s$, estesa per linearità. f è surgettiva in quanto l'immagine contiene un insieme di generatori di M, e dunque tutto M. Quindi $M = A^S/\ker(f)$, ovvero ogni A-modulo è quoziente di un A-modulo libero. Il nucleo di f dà le relazioni tra i generatori di M.

Proposizione 3.2. Sia M un A-modulo ed S un insieme di generatori di M. S è libero se e solo se per ogni A-modulo N e per ogni funzione $f : S \longrightarrow N$, $\exists! \tilde{f} : M \longrightarrow N$ omomorfismo di A-moduli tale che $\tilde{f}|_S = f$. In particolare, è sempre possibile definire un omomorfismo su una base di un modulo libero M ed estenderlo per linearità a tutto M.

Dimostrazione. ($\Longrightarrow$) Data $f : S \longrightarrow N$, se $\tilde{f}$ deve essere un omomorfismo che estende f, allora, preso $m \in M,\ m = \sum a_i s_i,\ a_i \in A,\ s_i \in S$, quindi $\tilde{f}(m) = \tilde{f}(\sum a_i s_i) = \sum a_i \tilde{f}(s_i) = \sum a_i f(s_i)$. Dunque $\tilde{f}$ è univocamente determinato da f. Inoltre questa definizione di f dà effettivamente un omomorfismo, perché la scrittura di m come combinazione lineare degli s_i è unica in quanto S è libero.

($\Longleftarrow$) Sia $N = A^S$, e sia $f : S \longrightarrow A^S,\ s \mapsto e_s$. Per ipotesi f si estende a un omomorfismo $\tilde{f} : M \longrightarrow A^S$. $\tilde{f}$ è surgettivo poiché l'immagine di $\tilde{f}$ contiene tutti gli e_s, che generano A^S. Inoltre, se $m = \sum a_i s_i \in \ker(\tilde{f}),\ 0 = \tilde{f}(\sum a_i s_i) = \sum a_i \tilde{f}(s_i) = \sum a_i e_{s_i}$. Poiché A^S è libero, si deve avere $a_i = 0\ \forall i$, cioè $m = 0$. $\tilde{f}$ è anche iniettiva, quindi un isomorfismo, che implica che anche M è libero.

□

Esempio. *Sia A un anello e x un'indeterminata. Per ogni $i \in \mathbb{N}$ definiamo $M_i = \langle x^i \rangle_A$. Ciascun M_i si immerge in $A[x]$, e in realtà $\bigoplus_{i \in \mathbb{N}} M_i \cong A[x]$ (i polinomi hanno solo un numero finito di coefficienti diversi da 0). Invece $A[[x]]$ si proietta su ciascun M_i nel seguente modo: $\sum a_n x^n \mapsto a_i x_i$. E in effetti $\prod_{i \in \mathbb{N}} M_i \cong A[[x]]$.*

Più in generale, dati degli A-moduli $M_h,\ N$, e mappe $f_h : M_h \longrightarrow N$, $\exists! f : \bigoplus M_h \longrightarrow N$ tale che $\forall h\ f \circ i_h = f_h$, dove i_h è l'inclusione di M_h nella somma diretta: questa è nota come la *proprietà universale della somma diretta*. Una proprietà simile vale per il prodotto diretto, ma con tutte le frecce invertite: date $g_h : N \longrightarrow M_h,\ \exists! g : N \longrightarrow \prod M_h$ tale che $\pi_h \circ g = g_h$, dove π_h è la proiezione su M_h.

Dimostriamo, per esempio, la proprietà universale della somma diretta. Osserviamo che, se f soddisfa la proprietà voluta, e $m = (m_h)_h \in \bigoplus M_h$, con un numero finito di m_h non nulli, si può scrivere $m = \sum_{h \in H} i_h(m_h)$, dove $i_h(m_h)$ ha m_h alla coordinata h e 0 altrove, e quindi $f(m) = f(\sum_{h \in H} i_h(m_h)) = \sum_{h \in H} f_h(m_h)$, dunque le f_h determinano univocamente f. D'altro canto

$$f : \bigoplus_{h \in H} M_h \longrightarrow N,\ (m_h)_{h \in H} \mapsto \sum_{h \in H} f_h(m_h)$$

è la funzione cercata: infatti è un omomorfismo in quanto somma di omomorfismi, e $f(i_h(m_h)) = f_h(m_h)$ per definizione di i_h e di f.

3.3 Lemma di Nakayama

In questa sezione dimostreremo il lemma di Nakayama, uno strumento molto utile con conseguenze importanti. Iniziamo con una versione generalizzata di un teorema già noto per gli spazi vettoriali, il teorema di Cayley-Hamilton.

Teorema 3.3 (Cayley-Hamilton)**.** Sia M un A-modulo *finitamente generato*, sia I un ideale di A e sia $\varphi \in \mathrm{End}_A(M) : \varphi(M) \subseteq IM$. Allora $\exists a_0, ..., a_{n-1} \in I : \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0\varphi^0 \equiv 0$. (Ricordiamo che φ^k è φ applicato k volte, e che φ^0 è l'identità su M).

Dimostrazione. Sia $M = \langle m_1, ..., m_n \rangle_A$. Poiché $\varphi(M) \subseteq IM,\ \varphi(m_i) = \sum c_k n_k$, $c_k \in I,\ n_k \in M$. Espandendo gli n_k rispetto a $m_1, \cdots, m_n$, si ottiene $\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$, con $a_{ij} \in I$. Dunque $\varphi(m_1, ..., m_n)^T = (a_{ij})_{i,j}(m_1, ..., m_n)^T$, e gli a_{ij} formano una matrice[4] $n \times n$. Se chiamiamo A questa matrice, allora abbiamo $(\varphi I - A)(m_1, ..., m_n)^T = 0$, dove I è la matrice identità $n \times n$ ($\varphi I - A$ è una matrice a coefficienti in $A[\varphi]$). Moltiplicando entrambi i membri per l'aggiunta di $\varphi I - A$ si ottiene $\det(\varphi I - A)(m_1, ..., m_n)^T = 0$. Poiché gli m_i generano M e la funzione $\det(\varphi I - A)$ si annulla su di essi, $\det(\varphi I - A)$ è l'endomorfismo nullo. Poiché le entrate di A stanno in I, $\det(\varphi I - A)$ è un polinomio monico in φ i cui coefficienti, escluso quello di testa, appartengono a I, come voluto. □

Prima di enunciare il lemma di Nakayama, vediamo un'interessante applicazione del teorema di Cayley-Hamilton, che generalizza un risultato già noto per spazi vettoriali ai moduli liberi.

Proposizione 3.4. Sia A un anello, ed $m, n \in \mathbb{N}$.

1. Se $f : A^m \longrightarrow A^n$ è surgettiva, allora $m \geq n$.
2. Se $f : A^m \longrightarrow A^n$ è iniettiva, allora $m \leq n$.
3. Se $f : A^m \longrightarrow A^n$ è un isomorfismo, allora $m = n$.

Dimostrazione. La 3 segue immediatamente dalle prime due.

1. Supponiamo per assurdo che $m < n$. Sia $\pi : A^n \longrightarrow A^m$ la proiezione sulle prime m coordinate in A^n. Allora $\pi \circ f : A^m \longrightarrow A^m$ è surgettiva, e un endomorfismo surgettivo di A^m è un isomorfismo (lo dimostreremo a breve). Questo è assurdo, in quanto $\ker \pi$ è non banale ed f è surgettiva: preso $0 \neq x \in \ker \pi,\ x = f(y)$ per qualche $y \neq 0$, e $\pi(f(y)) = 0$.
2. Supponiamo per assurdo che $m > n$. Sia $i : A^n \longrightarrow A^m$ l'inclusione, $i(a_1, ..., a_n) = i(a_1, ..., a_n, 0, ..., 0)$. Allora $\varphi = i \circ f$ è un endomorfismo iniettivo di A^m. Applichiamo il teorema di Cayley-Hamilton con $I = A$: la condizione su $\varphi(M)$ è automaticamente verificata, ed esistono $a_0, ..., a_{k-1} \in A$

[4] Tale matrice non è necessariamente unica, in quanto gli m_i potrebbero essere linearmente dipendenti.

tali che $\varphi^k + a_{k-1}\varphi^{k-1} + \cdots + a_0 \,\mathrm{id}_{A^m} \equiv 0$. Prendiamo il minimo valore di k per cui ciò accade. Allora $a_0 \neq 0$: infatti, se $a_0 = 0$, avremmo $\varphi \circ [\varphi^{k-1} + a_{k_1}\varphi^{k-2} + \cdots + a_1] = 0$, cioè $\mathrm{Im}(\varphi^{k-1} + a_{k-1}\varphi^{k-2} + \cdots + a_1) \subseteq \ker \varphi = 0$ e $\varphi^{k-1} + a_{k-1}\varphi^{k-2} + \cdots + a_1 = 0$, contraddicendo la minimalità di k. Sia e_m l'm-esimo elemento della base canonica di A^m, (0,...,0,1). Si ha

$$0 = (\varphi^k + a_{k-1}\varphi^{k-1} + \cdots + a_0)(e_m) =$$

$$a_0 e_m + \varphi((\varphi^{k-1} + a_{k-1}\varphi^{k-2} + \cdots + a_1)(e_m)) = a_0 e_m + \varphi(v).$$

Poiché $\varphi = i \circ f$, $\varphi(v) \in \mathrm{Im}\, i$, quindi $\varphi(v)$ ha l'ultima coordinata nulla $(m > n)$. Ma allora l'ultima coordinata di $(\varphi^k + a_{k_1}\varphi^{k-1} + \cdots + a_0)(e_m) = a_0 e_m + \varphi(v)$ è $a_0 \neq 0$, assurdo.

□

Lemma 3.5. (Nakayama) Sia M un A-modulo finitamente generato, e sia I un ideale di A.

1. Se $M = IM$, allora $\exists a \in A : a \equiv 1 \pmod{I}$ e $a \in \mathrm{Ann}(M)$.
2. Se $M = IM$ e $I \subseteq J(A)$, allora $M = 0$.
3. Se N è un sottomodulo di M tale che $M = N + IM$, con $I \subseteq J(A)$, allora $N = M$.

Dimostrazione. 1. Sia $\varphi = \mathrm{id}_M$. Abbiamo che $\varphi(M) = M = IM$. Per il teorema di Cayley-Hamilton, $\exists a_0, ..., a_{n-1} \in I : \mathrm{id}_M^n + a_{n-1}\,\mathrm{id}_M^{n-1} + \cdots + a_0 \equiv 0$. Dunque $(1 + a_{n-1} + \cdots + a_0)m = am = 0 \ \forall m \in M$. Gli a_i appartengono a I, quindi $a \equiv -1 \pmod{I}$ e $a \in \mathrm{Ann}(M)$. Anche $-a \in \mathrm{Ann}(M)$, e $-a \equiv 1 \pmod{I}$, da cui la tesi.

2. Poiché $M = IM$, per 1. esiste $a \in \mathrm{Ann}(M) : a \equiv 1 \pmod{I}$. Quindi $1 - a \in I$. Ma $I \subseteq J(A)$, e per la caratterizzazione di $J(A)$ $1 - (1 - a) = a \in A^*$. Essendo $aM = 0$, si deve avere $M = 0$.

3. Sia $f : N + IM \longrightarrow I(M/N),\ f(n + im) = i\overline{m} = \overline{im}$.

   - f è ben definita: se $n_1 + i_1 m_1 = n_2 + i_2 m_2$ sono due scritture diverse dello stesso elemento, allora $i_1 m_1 = i_2 m_2 + n_2 - n_1$, dove $n_1, n_2 \in N$, quindi $f(n_1 + i_1 m_1) = \overline{i_1 m_1} = \overline{i_2 m_2 + n_2 - n_1} = \overline{i_2 m_2} = f(n_2 + i_2 m_2)$.
   - f è un omomorfismo di A-moduli: $f((n_1 + i_1 m_1) + (n_2 + i_2 m_2)) = \overline{i_1 m_1 + i_2 m_2} = \overline{i_1 m_1} + \overline{i_2 m_2} = f(n_1 + i_1 m_1) + f(n_2 + i_2 m_2)$, $f(a(n + im)) = f(an + aim) = \overline{a(im)} = a\overline{im} = af(n + im)$.
   - f è surgettivo: $\forall i\overline{m} \in I(M/N) f(im) = i\overline{m}$.
   - $n + im \in \ker f$ se e solo se $\overline{im} = 0$, cioè $im \in N$, che equivale a $n + im \in N$. Quindi $\ker f = N$.

Per il primo teorema di isomorfismo $(N+IM)/N \cong I(M/N)$ (questo vale per tutti i moduli, non è stata usata ancora nessuna ipotesi). Ora, per ipotesi $M = N+IM$, dunque $M/N \cong I(M/N)$. Essendo M/N finitamente generato (è quoziente di M, che è f.g. per ipotesi), e $I \subseteq J(A)$, per 2. si conclude che $M/N = 0$, ossia $M = N$.

□

Osservazione. L'ipotesi che M sia finitamente generato è necessaria. Infatti, se $A = \mathbb{Z},\ M = \mathbb{Q},\ I = (n),\ n \neq 0$, vale $(n)\mathbb{Q} = \mathbb{Q}$, ma $\mathrm{Ann}(\mathbb{Q}) = 0$.

Corollario. Sia $(A, \mathfrak{m}, k)$ un anello locale ed M un A-modulo finitamente generato.

1. Se $\overline{m_1}, ..., \overline{m_n}$ generano $M/\mathfrak{m}M$ come k-spazio vettoriale, allora $m_1, ..., m_n$ generano M come A-modulo.

2. Ogni insieme minimale di generatori di M ha la stessa cardinalità. Questo ci permette di definire il rango di M (modulo finitamente generato su anello locale) come la cardinalità di un qualunque insieme di generatori minimale di M.

Dimostrazione.

1. Sia $N = \langle m_1, ..., m_n \rangle_A \subseteq M$. M è finitamente generato e, per ipotesi, $M = N + \mathfrak{m}M$, quindi per Nakayama $N = M$.

2. Sia $m_1, ..., m_n$ un insieme di generatori minimale di M. Allora $\overline{m_1}, ..., \overline{m_n}$ generano $M/\mathfrak{m}M$, che è dunque uno spazio vettoriale su k di dimensione finita. Più precisamente, $\dim_k(M/\mathfrak{m}M) \leq n$. Supponiamo per assurdo che $\dim_k(M/\mathfrak{m}M) < n$. Allora da $m_1, ..., m_n$ possiamo estrarre una base di $M/\mathfrak{m}M,\ \{m_{i_1}, ..., m_{i_r}\},\ r < n$. Per il punto 1, $m_{i_1}, ..., m_{i_r}$ generano M, contraddicendo la minimalità di $m_1, ..., m_n$. Quindi $\dim_k(M/\mathfrak{m}M) = n$, e qualunque sistema di generatori minimale di M ha cardinalità n, in quanto corrisponde a una base del k-spazio vettoriale $M/\mathfrak{m}M$, e le basi degli spazi vettoriali di dimensione finita hanno sempre lo stesso numero di elementi.

□

Proposizione 3.6. Sia M un A-modulo finitamente generato, e sia f un endomorfismo di M surgettivo. Allora f è un isomorfismo.

Dimostrazione. Definiamo su M una struttura di $A[x]$-modulo, tramite l'azione $\cdot : A[x] \times M \longrightarrow M,\ p(x) \cdot m = (p(f))(m)$. Poiché f è surgettiva, $f(M) = M$, cioè $x \cdot M = M$, ovvero $(x)M = M$. In più M è f.g. anche come $A[x]$-modulo, perché l'azione di $A[x]$ ristretta ad A induce su M la sua struttura di A-modulo originaria,[5] quindi, se $m_1, ..., m_n$ generano M come A-modulo, lo generano anche come $A[x]$-modulo. Per il lemma di Nakayama, $\exists p(x) \in \mathrm{Ann}(M) : p(x) \equiv 1 \pmod{(x)}$. Scriviamo $p(x) = 1 + xq(x)$. Sia ora $m \in \ker(f)$ e mostriamo che $m = 0$. Poiché $p(x)M = 0$, abbiamo $0 = p(x) \cdot m = (1 + q(x)x) \cdot m = m + (q(f))(f(m)) = m + (q(f))(0) = m$. Quindi f è iniettiva. Essendo f surgettiva per ipotesi, è un isomorfismo.

[5] Se $a \in A,\ (a(f))(m) = am$.

□

Osservazione. 1. Lo stesso non vale se supponiamo solo che f sia iniettiva: per esempio, se A è un anello qualunque (che non sia un campo), allora A è un A-modulo finitamente generato. Ma $a : A \longrightarrow A,\ b \mapsto ab$, con a non un'unità e non un divisore di zero, è iniettiva (a non divisore di zero) ma non surgettiva (a non invertibile).

2. La proposizione non vale se M non è finitamente generato. Infatti, se $M = A^{\mathbb{N}} = A_0 \oplus A_1 \oplus ...$, con $A_i \cong A\ \forall i \in \mathbb{N}$, ed $N = A_0 \oplus 0 \oplus 0 \oplus ...$, allora $M/N \cong A^{\mathbb{N}} = M$, quindi la proiezione su M/N, composta con l'isomorfismo con M, è un endomorfismo surgettivo di M che non è iniettivo.

3.4 Successioni esatte

Definiamo un altro importante strumento per lo studio dei moduli, le successioni esatte, che ci permettono di dedurre le proprietà di un modulo M da "pezzi" più piccoli che compongono M.

Definizione (Complesso)**.** Un **complesso** di A-moduli è una famiglia $\{M_i, f_i\}_{i\in\mathbb{Z}}$ di A-moduli M_i e di omomorfismi $f_i : M_i \longrightarrow M_{i+1}$ tali che, $\forall i \in \mathbb{Z},\ f_{i+1} \circ f_i = 0$, cioè $\mathrm{Im}(f_i) \subseteq \ker(f_{i+1})$. La notazione per un complesso è la seguente:

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

Tale complesso si dice **esatto** se $\forall i \in \mathbb{Z}\ \mathrm{Im}(f_i) = \ker(f_{i+1})$.

Definizione (Successione esatta corta)**.** Una **successione esatta corta** è un complesso esatto con al più 3 elementi diversi da 0. La notazione è

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0.$$

(Ci sarebbero infiniti moduli nulli da ambo i lati, ma non aggiungono ulteriori informazioni e possono essere ignorati).

L'esattezza della successione in M significa che l'immagine di $0 \hookrightarrow M$ è uguale a $\ker(f)$, cioè che $\ker(f) = 0$, ossia che f è iniettiva. Similmente, l'esattezza in P equivale a $\mathrm{Im}(g) = \ker(P \longrightarrow 0) = P$, cioè alla surgettività di g. L'esattezza in N, la condizione principale, è per definizione $\mathrm{Im}(f) = \ker(g)$. Un esempio semplice è $0 \longrightarrow A^n \longrightarrow A^{n+l} \longrightarrow A^l \longrightarrow 0$, per qualunque anello A. Si osserva facilmente che $A^{n+l} \cong A^n \oplus A^l$. Più in generale, se M, N sono A-moduli, $0 \to M \xrightarrow{i} M \oplus N \xrightarrow{\pi} N \to 0$ è una successione esatta corta: infatti, l'inclusione di M in $M \oplus N$ è iniettiva, la proiezione di $M \oplus N$ su N è surgettiva, e $\ker \pi = \mathrm{Im}\, i = M$. Non tutte le successioni esatte corte sono di questa forma: per esempio, la successione di $\mathbb{Z}$-moduli

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(2) \to 0$$

è esatta, ma $\mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z}/(2)$. (La mappa da $\mathbb{Z}$ in $\mathbb{Z}$ è moltiplicazione per 2). Questa successione è un controesempio a molte "buone" proprietà delle successioni esatte.

La prossima proposizione mostra un esempio esplicito in cui si può dedurre una proprietà dell'elemento centrale di una successione esatta corta dagli elementi laterali.

Proposizione 3.7. Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ una successione esatta corta di A-moduli. Allora tutti i sottomoduli di N sono finitamente generati[6] se e solo se tutti i sottomoduli di M e di P sono finitamente generati.

Dimostrazione. ($\Longrightarrow$) Se H è un sottomodulo di M, $f(H)$ è un sottomodulo di N ed è quindi f.g. per ipotesi. Poiché f è iniettiva, H è isomorfo a $f(H)$, dunque è finitamente generato. Se L è un sottomodulo di P, $g^{-1}(L)$ è un sottomodulo di N, dunque è f.g.. Allora le immagini dei generatori di $g^{-1}(L)$ generano L.

($\Longleftarrow$) Sia H un sottomodulo di N. Allora $H \cap f(M)$ è un sottomodulo di $f(M)$, che è isomorfo a M in quanto f è iniettiva, dunque $H \cap f(M)$ è f.g. per ipotesi. Siano $h_1, ..., h_r$ i suoi generatori. Allo stesso modo, $g(H)$ è un sottomodulo di P ed è quindi f.g.. Siano $g(h_{r+1}), ..., g(h_n)$ i suoi generatori. Possiamo assumere $h_{r+1}, ..., h_n$ distinti da $h_1, ..., h_r$ in quanto, se $h_i = h_j,\ i \leq r < j$, allora $h_j \in f(M) \implies g(h_j) \in g(f(M)) = 0$, poiché in un complesso (esatto o meno) la composizione di due mappe successive fa 0. Ora dimostriamo che $H = \langle h_1, ..., h_n \rangle_A$. Sia $h \in H$. $g(H)$ è generato da $h_{r+1}, ..., h_n$, quindi $g(h) = \sum_{i=r+1}^{n} a_i g(h_i) = g(\sum_{i=r+1}^{n} a_i h_i)$. Poiché h e $\sum_{i=r+1}^{n} a_i h_i$ hanno la stessa immagine tramite g, $h - \sum_{i=r+1}^{n} a_i h_i \in \ker g = \operatorname{Im} f$, essendo la successione esatta. Inoltre è chiaro che $h - \sum_{i=r+1}^{n} a_i h_i \in H$, dunque $h - \sum_{i=r+1}^{n} a_i h_i \in H \cap f(M)$, che è generato da $h_1, ..., h_r$. Si può allora scrivere $h - \sum_{i=r+1}^{n} a_i h_i = \sum_{i=1}^{r} a_i h_i \implies h = \sum_{i=1}^{n} a_i h_i$. □

Data una successione esatta $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$, vogliamo capire sotto quali condizioni $N \cong M \oplus P$. In questo caso, si dice che la successione **spezza** (*splits*).

Teorema 3.8. Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ una successione esatta corta. I seguenti fatti sono equivalenti:

1. $\exists \eta : N \longrightarrow M : \eta \circ f = \mathrm{id}_M$ (η è detta *retrazione* di f);
2. $\exists \lambda : P \longrightarrow M : g \circ \lambda = \mathrm{id}_P$ (λ è detta *sezione* di g);

[6] Se N ha questa proprietà, si dice che N è un modulo *noetheriano*. Quindi la proposizione afferma che N è noetheriano se e solo se M e P sono noetheriani.

3. $\exists \nu : N \longrightarrow M \oplus P$ isomorfismo tale che il diagramma

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \mathrm{id}_P} & & \\
0 & \longrightarrow & M & \xrightarrow{i_M} & M \oplus P & \xrightarrow{\pi_P} & P & \longrightarrow & 0
\end{array}$$

commuta.

Dimostrazione. ($1 \implies 2$) Step 1: $N = \operatorname{Im} f \oplus \ker \eta$. Sia $\alpha \in N$. Allora $\alpha = [\alpha - f(\eta(\alpha))] + f(\eta(\alpha))$. Il secondo addendo è chiaramente nell'immagine di f, e il primo addendo è in $\ker \eta$: $\eta(\alpha - f(\eta(\alpha))) = \eta(\alpha) - \eta(f(\eta(\alpha))) = \eta(\alpha) - \eta(\alpha) = 0$, usando il fatto che $\eta \circ f = \mathrm{id}_M$. Quindi $N = \operatorname{Im} f + \ker \eta$. Per mostrare che la somma è diretta, serve l'ulteriore condizione che $\operatorname{Im} f \cap \ker \eta = 0$. Se $\alpha \in \operatorname{Im} f \cap \ker \eta,\ \alpha = f(\beta)$ per qualche $\beta \in M$, e $0 = \eta(\alpha) = \eta(f(\beta)) = \beta \implies \alpha = f(\beta) = 0$.

Step 2: costruzione di λ. Poiché g è surgettiva, dato $p \in P\ \exists \alpha \in N : g(\alpha) = p$. Poniamo $\lambda(p) = \alpha - f(\eta(\alpha))$.

- λ è ben definita: se $\alpha_1, \alpha_2 \in N$ con $g(\alpha_1) = g(\alpha_2),\ \alpha_1 - \alpha_2 \in \ker g = \operatorname{Im} f$. Sia $\beta \in M : f(\beta) = \alpha_1 - \alpha_2$. Allora $\lambda(\alpha_1) - \lambda(\alpha_2) = \alpha_1 - f(\eta(\alpha_1)) - \alpha_2 + f(\eta(\alpha_2)) = f(\beta) - f(\eta(\alpha_1 - \alpha_2)) = f(\beta) - f(\eta(f(\beta))) = f(\beta) - f(\beta) = 0$.
- λ è un omomorfismo: ovvio, in quanto è definito da somme e composizione di omomorfismi.
- $g \circ \lambda = \mathrm{id}_P$: se $p \in P,\ g(\lambda(p)) = g(\alpha - f(\eta(\alpha)))$, dove $g(\alpha) = p$. Quindi $g(\lambda(p)) = g(\alpha) - g(f(\eta(\alpha))) = g(\alpha) = p$, in quanto $g \circ f = 0$.

($2 \implies 1$) Dimostrazione analoga. In questo caso si mostra che $N = \operatorname{Im} \lambda \oplus \ker g$.

($1 \implies 3$) Definiamo $\nu : N \longrightarrow M \oplus P,\ \nu(\alpha) = (\eta(\alpha), g(\alpha))$, e mostriamo che è l'isomorfismo cercato.

- ν omomorfismo: ovvio.
- ν iniettivo: $\alpha \in \ker \nu \iff \alpha \in \ker \eta \cap \ker g = \ker \eta \cap \operatorname{Im} f$. Poiché $\ker \eta$ e $\operatorname{Im} f$ sono in somma diretta sotto le ipotesi di 1, come mostrato sopra, $\alpha = 0$.
- ν surgettivo: sia $(m, p) \in M \oplus P$. Prendiamo $\alpha \in N : g(\alpha) = p$, sfruttando la surgettività di g, e poniamo $\beta = \alpha - f(\eta(\alpha)) + f(m)$. Si ha $g(\beta) = g(\alpha) - g(f(\eta(\alpha))) + g(f(m)) = p,\ \eta(\beta) = \eta(\alpha) - \eta(f(\eta(\alpha))) + \eta(f(m)) = \eta(\alpha) - \eta(\alpha) + m = m$.
- ν fa commutare il diagramma: dobbiamo mostrare che $\nu \circ f = \pi_M,\ \pi_P \circ \nu = g$. Per la prima, abbiamo $\nu(f(m)) = (\eta(f(m)), g(f(m))) = (m, 0) = i_M(m)$. Per la seconda, abbiamo $\pi_P(\nu(n)) = \pi_P(\eta(n), g(n)) = g(n)$.

$(3 \Longrightarrow 1)$ Sia $\eta : N \longrightarrow M,\ \eta(\alpha) = \pi_M(\nu(\alpha))$. η è un omomorfismo, e inoltre $\forall m \in M\ \eta(f(m)) = \pi_M(\nu(f(m)) = \pi_M(i_M(m)) = m$.

□

Osservazione. Se la successione esatta $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ spezza, date $\eta,\ \lambda$ come nel teorema precedente, anche la successione $0 \to P \xrightarrow{\lambda} N \xrightarrow{\eta} M \to 0$ è esatta e spezza. Infatti, è esatta poiché λ è iniettiva, avendo g come inversa sinistra, η è surgettiva, avendo f come inversa destra, e infine $N = \operatorname{Im} f \oplus \ker \eta = \operatorname{Im} \lambda \oplus \ker g$, e dato che $\operatorname{Im} f = \ker g$, si ha anche $\operatorname{Im} \lambda = \ker \eta$. Inoltre, la successione spezza perché g è una retrazione di λ, ed f è una sezione di η. Si potrebbe dire che c'è una "dualità" fra retrazioni e sezioni.

Vogliamo ora dimostrare un risultato classico, noto come *lemma del serpente*. Premettiamo due osservazioni.

1. Consideriamo il complesso $\cdots \longrightarrow 0 \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} 0 \longrightarrow \cdots$, e supponiamo che il complesso sia esatto in M_i. Allora $\ker f_i = \operatorname{Im} f_{i-1} = 0$, e l'immagine di f_i è 0, cioè $\ker f_i = M_i$. Dunque $M_i = 0$.

2. Dato un omomorfismo di A-moduli $f : M \longrightarrow N$, si ottiene una successione esatta a 4 pezzi:

$$0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0.$$

   L'esattezza deriva dal fatto che $\ker f$ è un sottomodulo di M, $\operatorname{coker} f$ è un quoziente di N, $\ker f$ è l'immagine della sua immersione in M e $\operatorname{Im} f$ è il nucleo della proiezione di N su $\operatorname{coker} f$.

Proposizione 3.9 (Lemma del serpente)**.** Consideriamo il diagramma commutativo

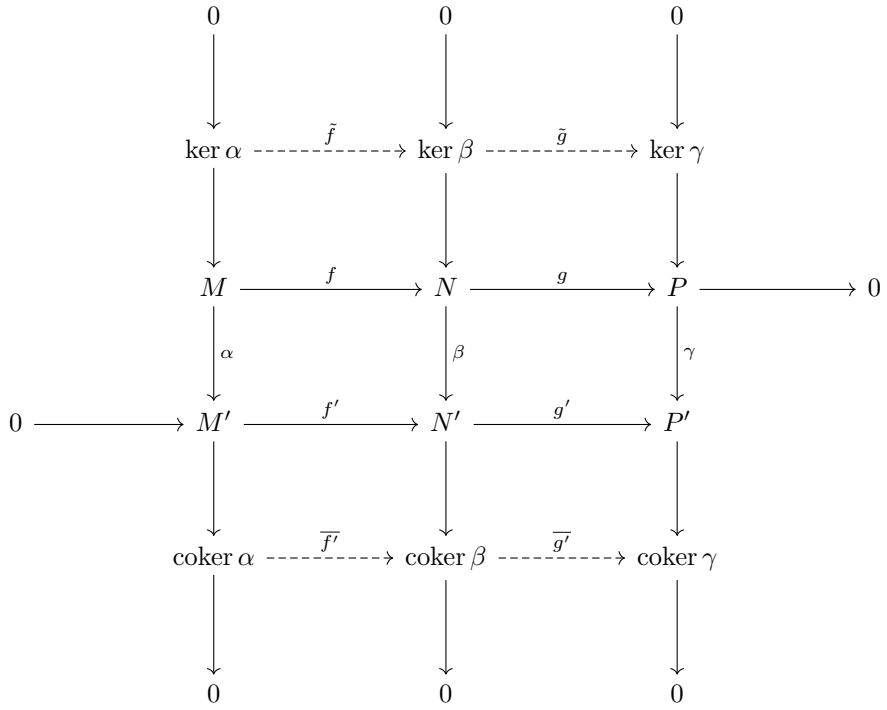
$$\begin{array}{ccccccccc} & & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{f'} & N' & \xrightarrow{g'} & P' & & \end{array}$$

le cui righe sono esatte. Allora c'è una successione esatta

$$\ker \alpha \to \ker \beta \to \ker \gamma \to \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma.$$

Inoltre, se f è iniettiva, lo è anche $\ker \alpha \to \ker \beta$; se g' è surgettiva, lo è anche $\operatorname{coker} \beta \to \operatorname{coker} \gamma$.

Dimostrazione. Usiamo l'osservazione precedente per costruire il diagramma



Dobbiamo definire le mappe tratteggiate, e in più una funzione da $\ker\gamma$ a $\operatorname{coker}\alpha$, in modo da far commutare tutto il diagramma.

Step 1: costruzione delle mappe tratteggiate. Definiamo $\tilde{f} = f|_{\ker\alpha}$, $\tilde{g} = g|_{\ker\beta}$, $\overline{f'}(\overline{m'}) = \overline{f'(m')}$, $\overline{g'}(\overline{n'}) = \overline{g'(n')}$, in modo tale che tutti i quadrati commutino. Verifichiamo che $\tilde{f}$ è ben definita, ovvero che è effettivamente a valori in $\ker\beta$: se $m \in \ker\alpha$, $\beta(\tilde{f}(m)) = \beta(f(m)) = f'(\alpha(m)) = 0$ in quanto $m \in \ker\alpha$ e $\beta \circ f = f' \circ \alpha$. Analogamente si dimostra che $\tilde{g}$ è ben definita. Dimostriamo ora che $\overline{f'}$ è ben definita: è sicuramente a valori in $\operatorname{coker}\beta$, ma è definita su un quoziente. Se $m_1', m_2' \in M'$ rappresentano lo stesso elemento di $\operatorname{coker}\alpha$, la loro differenza, $m_1' - m_2'$, sta in $\operatorname{Im}\alpha$. Sia dunque $m \in M$: $\alpha(m) = m_1' - m_2'$; allora $\overline{f'}(\overline{m_1'}) - \overline{f'}(\overline{m_2'}) = \overline{f'(m_1')} - \overline{f'(m_2')} = \overline{f'(m_1' - m_2')} = \overline{f'(\alpha(m))} = \overline{\beta(f(m))} = \overline{0}$, perché $\beta(f(m))$ è 0 in $\operatorname{coker}\beta$. Allo stesso modo si dimostra che $\overline{g'}$ è ben definita.

Step 2: costruzione di δ. Vogliamo definire una mappa[7] $\delta : \ker\gamma \longrightarrow \operatorname{coker}\alpha$, e la strategia sarà di seguire uno zig-zag nel diagramma. Sia $p \in \ker\gamma \subseteq P$. g è surgettiva, quindi $\exists n \in N : g(n) = p$. Prendiamo l'immagine $\beta(n) \in N'$; a questo punto vorremmo rimontarla a un elemento di M'. Ci serve che $\beta(n) \in \operatorname{Im} f'$, che per esattezza coincide con $\ker g'$. Poiché $g'(\beta(n)) = \gamma(g(n)) = \gamma(p) = 0$ (ricordando che $g(n) = p$ e $p \in \ker\gamma$), concludiamo che esiste $m \in M'$ tale che

[7] δ è chiamata a volte *omomorfismo connettivo*, o anche *snake map*, perché assomiglia a un serpente che si snoda da $\ker\gamma$ a $\operatorname{coker}\alpha$, e dà il nome al "lemma del serpente".

$f'(m) = \beta(n)$. Inoltre tale m è unico per l'iniettività di f'. Infine proiettiamo m a $\overline{m} \in \operatorname{coker}\alpha$, e definiamo $\delta(p) = \overline{m}$. Resta da verificare la buona definizione di δ, che *a priori* potrebbe dipendere dalla scelta di n. Siano dunque $n, n' \in N : g(n) = g(n') = p$, e siano $m, m' \in M' : f'(m) = \beta(n),\ f'(m') = \beta(n')$. Dobbiamo mostrare che $\overline{m} = \overline{m'}$, cioè che $m - m' \in \operatorname{Im}\alpha$. $g(n) = g(n') = p \implies n - n' \in \ker g = \operatorname{Im} f$. Sia $u \in M : f(u) = n - n'$; applicando β a entrambi i membri otteniamo $\beta(f(u)) = \beta(n - n') = f'(m - m')$. Osserviamo che $\beta \circ f = f' \circ \alpha$, dunque $f'(m - m') = f'(\alpha(u))$. Ma f' è iniettiva, quindi $m - m' = \alpha(u)$, come voluto.

Step 3: esattezza della successione. Abbiamo dimostrato che la successione

$$\ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma$$

esiste; ora mostriamo che è esatta. Le dimostrazioni di questo tipo di enunciati sono molto simili tra loro, e utilizzano la tecnica del *diagram chasing* (in pratica, "seguire le frecce"). Noi ne illustriamo qualche esempio.

- Esattezza in $\ker\alpha$ (nel caso in cui f è iniettiva): basta notare che $\tilde{f}$ è iniettiva in quanto restrizione di iniettiva.
- Esattezza in $\ker\beta$: dobbiamo mostrare che $\ker\tilde{g} = \operatorname{Im}\tilde{f}$. Se $m \in \ker\alpha$, $\tilde{g}(\tilde{f}(m)) = g(f(m)) = 0$, quindi $\ker\tilde{g} \supseteq \operatorname{Im}\tilde{f}$. Sia ora $n \in \ker\tilde{g} = \ker g \cap \ker\beta$. Per le ipotesi di esattezza $\ker g = \operatorname{Im} f$, ossia $\exists m \in M : f(m) = n$. È sufficiente mostrare che $m \in \ker\alpha$: osserviamo che $f'(\alpha(m)) = \beta(f(m)) = \beta(n) = 0$, e per iniettività di f' $\alpha(m) = 0$.
- Esattezza in $\operatorname{coker}\alpha$: sia $p \in \ker\gamma,\ p = g(n),\ \beta(n) = f'(m)$; allora $\delta(p) = \overline{m}$. Quindi $\overline{f'}(\delta(p)) = \overline{f'}(\overline{m}) = \overline{f'(m)} = \overline{\beta(n)} = 0$ in $\operatorname{coker}\beta$. Dunque $\operatorname{Im}\delta \subseteq \ker\overline{f'}$. Se invece $\overline{m} \in \ker\overline{f'},\ \overline{f'(m)} = 0$, cioè $f'(m) \in \operatorname{Im}\beta$. Sia $n \in N : \beta(n) = f'(m)\, p = g(n)$; se $p \in \ker\gamma,\ \overline{m} = \delta(p)$ e abbiamo concluso. Si ha $\gamma(p) = \gamma(g(n)) = g'(\beta(n)) = g'(f'(m)) = 0$, come voluto.

□

Corollario. Dato il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & P' & \longrightarrow & 0 \end{array}$$

con righe esatte, se due delle tre frecce verticali sono isomorfismi, anche la terza lo è.

Dimostrazione. Usando le stesse notazioni di prima, per il lemma del serpente c'è una successione esatta

$$0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0.$$

Se due tra α, β, γ sono isomorfismi, essi hanno sia nucleo che conucleo nulli, quindi il nucleo e il conucleo della mappa rimanente sono schiacciati tra due 0 in una successione esatta, e per l'osservazione preliminare devono essere 0, ovvero la terza mappa è anch'essa un isomorfismo.

□

3.5 Il funtore $\mathrm{Hom}(M, \bullet)$

Continuiamo a studiare il problema delle successioni che spezzano, analizzandolo da un punto di vista più astratto, e introducendo il linguaggio delle categorie e dei funtori.

Siano M, N, P A-moduli, e fissiamo un omomorfismo $g : N \longrightarrow P$. Allora g induce una mappa tra $\mathrm{Hom}(M, N)$ e $\mathrm{Hom}(M, P)$ nel seguente modo: preso $\varphi \in \mathrm{Hom}(M, N),\ g \circ \varphi \in \mathrm{Hom}(M, P)$. Abbiamo effettivamente definito una "funzione" che manda A-moduli in A-moduli. La "famiglia" degli A-moduli è un esempio di una *categoria*, e questa "funzione" $F : A\text{-moduli} \longrightarrow A\text{-moduli}$, $N \mapsto \mathrm{Hom}(M, N)$ è detta *funtore*. La proprietà cardine di un funtore è che, oltre a trasformare gli "oggetti" di una categoria, nel nostro caso A-moduli, trasforma anche i "morfismi" tra gli oggetti (omomorfismi di A-moduli). Nel nostro caso, $F(N) = \mathrm{Hom}(M, N)$ associa a ogni omomorfismo g tra N e P l'omomorfismo $F(g) = g_* : \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M, P),\ g_*(\varphi) = g \circ \varphi$. Un funtore, per essere definito tale, deve godere di due proprietà:

1. $F(\mathrm{id}_N) = \mathrm{id}_{F(N)}$;
2. $F(h \circ g) = F(h) \circ F(g)$.

Nel nostro caso, osserviamo che $F(\mathrm{id}_N)(\varphi) = \mathrm{id}_{N_*}(\varphi) = \mathrm{id}_N \circ \varphi = \varphi\ \forall \varphi \in \mathrm{Hom}(M, N)$, e $F(h \circ g)(\varphi) = (h \circ g)_*(\varphi) = (h \circ g) \circ \varphi = h \circ (g \circ \varphi) = h \circ g_*(\varphi) = h_*(g_*(\varphi))\ \forall \varphi \in \mathrm{Hom}(M, N),\ g \in \mathrm{Hom}(N, P),\ h \in \mathrm{Hom}(P, L)$.

Riassumendo, abbiamo definito il funtore $N \mapsto \mathrm{Hom}(M, N)$, che a ogni omomorfismo $g : N \longrightarrow P$ associa $g_* : \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M, P)$. Questo funtore "rispetta i versi delle frecce", ed è quindi detto funtore *covariante*.

Se M, N, P sono A-moduli, e $g \in \mathrm{Hom}(N, P),\ g$ induce anche una mappa tra $\mathrm{Hom}(P, M)$ e $\mathrm{Hom}(N, M)$, mandando φ in $g^*(\varphi) = \varphi \circ g$. Si può dimostrare allo stesso modo che anche $N \longrightarrow \mathrm{Hom}(N, M)$ è un funtore. Ma in questo caso, a $g : N \longrightarrow P$ corrisponde $g^* : \mathrm{Hom}(P, M) \longrightarrow \mathrm{Hom}(N, M)$: il verso della freccia è stato invertito. In tal caso si parla di funtore *controvariante*.

Il prossimo risultato mostra come interagisce il funtore $\mathrm{Hom}(M, \bullet)$ con le successioni esatte.

Teorema 3.10. La successione di A-moduli $0 \to N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ è esatta se e solo se, per ogni A-modulo M, la successione $0 \to \mathrm{Hom}(M, N_1) \xrightarrow{f_*} \mathrm{Hom}(M, N) \xrightarrow{g_*} \mathrm{Hom}(M, N_2)$ è esatta.

Dimostrazione. ($\Longrightarrow$) Per l'esattezza in $\mathrm{Hom}(M, N_1)$ dobbiamo mostrare che f_* è iniettiva. Se $\varphi \in \ker f_*$, allora $f_*(\varphi) = f \circ \varphi$ è l'omomorfismo nullo, cioè

$\operatorname{Im}\varphi \subseteq \ker f = 0$ in quanto f è iniettiva. Quindi $\varphi \equiv 0$ e f_* è iniettiva. Per mostrare l'esattezza in $\operatorname{Hom}(M,N)$, serve che $\operatorname{Im} f_* = \ker g_*$. Per la funtorialità di $\operatorname{Hom}(M,\bullet)$, $g_* \circ f_* = (g \circ f)_* = 0_* = 0$, dunque $\operatorname{Im} f_* \subseteq \ker g_*$. Per il contenimento opposto, prendiamo $\psi \in \ker g_*$. Allora $g_*(\psi) = g \circ \psi = 0$, ovvero $\operatorname{Im}\psi \subseteq \ker g = \operatorname{Im} f$, in quanto la successione di partenza è esatta. Dunque ψ è un omomorfismo da M in N la cui immagine è contenuta nell'immagine di f, cioè $\forall m \in M\ \exists n_1 \in N_1$ tale che $\psi(m) = f(n_1)$. Inoltre, tale n_1 è unico per l'iniettività di f. Definiamo $\varphi : M \longrightarrow N_1$, $\varphi(m) = n_1$, dove n_1 è l'unico tale che $f(n_1) = \psi(m)$. Si ottiene che $f_*(\varphi)(m) = f(\varphi(m)) = f(n_1) = \psi(m)$, cioè $f_*(\varphi) = \psi$ e quindi $\psi \in \operatorname{Im} f_*$.

($\Longleftarrow$) Esattezza in N_1 : poniamo $M = \ker f$. Per ipotesi la successione $0 \to \operatorname{Hom}(M,N_1) \xrightarrow{f_*} \operatorname{Hom}(M,N) \xrightarrow{g_*} \operatorname{Hom}(M,N_2)$ è esatta, quindi f_* è iniettiva. Poiché $M = \ker f \subseteq N_1$, l'inclusione $i : M \hookrightarrow N_1$ è un elemento di $\operatorname{Hom}(M,N_1)$. Applicando f_* otteniamo $f_*(i)(m) = f(i(m)) = f(m) = 0$. Poiché f_* è iniettiva, si deve avere $i = 0$, ma anche i è iniettiva, quindi $\ker f = M = 0$, cioè f è iniettiva.

Esattezza in N: $(g \circ f)_* = g_* \circ f_* = 0$, quindi $g \circ f = 0$ e $\operatorname{Im} f \subseteq \ker g$. Per l'inclusione opposta, sia $M = \ker g$, che è un sottomodulo di N. Consideriamo $i : \ker g \hookrightarrow N$: abbiamo $g_*(i)(n) = g(i(n)) = g(n) = 0$, dunque $i \in \ker g_* = \operatorname{Im} f_*$. Allora esiste $\varphi : M \longrightarrow N_1$ tale che $i = f_*(\varphi) = f \circ \varphi$, e si deduce che $\ker g = \operatorname{Im} i \subseteq \operatorname{Im} f$.

□

Vale un enunciato simmetrico per il funtore $\operatorname{Hom}(\bullet, M)$ (ricordandosi di invertire il senso di tutte le frecce): la successione $0 \to N_1 \xrightarrow{f} N \xrightarrow{g} N_2$ è esatta se e solo se, per ogni A-modulo M, la successione $\operatorname{Hom}(N_2,M) \xrightarrow{g^*} \operatorname{Hom}(N,M) \xrightarrow{f^*} \operatorname{Hom}(N_1,M) \to 0$ è esatta.

Nel gergo della teoria delle categorie, si dice che $\operatorname{Hom}(M,\bullet)$ e $\operatorname{Hom}(\bullet,M)$ sono funtori *esatti a sinistra*, perché trasformano sucessioni esatte a sinistra in successioni esatte a sinistra. Più avanti vedremo esempi di funtori esatti a destra (prodotto tensoriale) e di funtori esatti sia a destra che a sinistra (localizzazione), detti semplicemente *esatti*.

ATTENZIONE: se $0 \to N_1 \xrightarrow{f} N \xrightarrow{g} N_2 \to 0$ è esatta, NON è sempre vero che $0 \to \operatorname{Hom}(M,N_1) \xrightarrow{f_*} \operatorname{Hom}(M,N) \xrightarrow{g_*} \operatorname{Hom}(M,N_2) \to 0$ è esatta! Per esempio, la successione $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(n) \to 0$ è esatta, ma $\operatorname{Hom}(\mathbb{Z}/(n),\mathbb{Z}) = 0$ (se $n \neq 0$), e $\operatorname{Hom}(\mathbb{Z}/(n),\mathbb{Z}/(n)) = \mathbb{Z}/(n)$, quindi non c'è modo che π_* sia surgettiva. Quindi il funtore $\operatorname{Hom}(M,\bullet)$ non è esatto a destra.

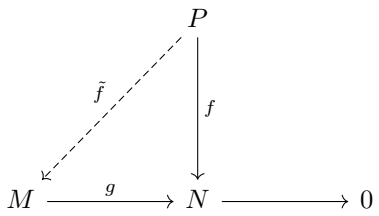
3.6 Moduli proiettivi e iniettivi

Abbiamo appena visto che $\operatorname{Hom}(M,\bullet)$ non è un funtore esatto a destra in generale, quindi cerchiamo di capire se esistono moduli M per i quali $\operatorname{Hom}(M,\bullet)$ è esatto.

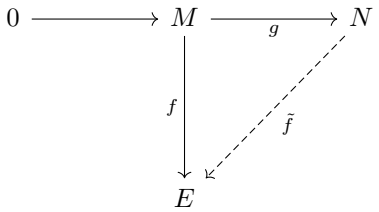
Definizione (Moduli proiettivi/iniettivi)**.** Sia A un anello e P, E A-moduli.

- P è **proiettivo** se il funtore $\mathrm{Hom}(P, \bullet)$ è esatto.
- E è **iniettivo** se $\mathrm{Hom}(\bullet, E)$ è esatto.

L'esempio precedente mostra che $\mathbb{Z}/(n)$ non è uno $\mathbb{Z}$-modulo proiettivo se $n \neq 0$. Cerchiamo di arrivare a una descrizione più esplicita dei moduli proiettivi. Poiché $\mathrm{Hom}(P, \bullet)$ è esatto a sinistra, dobbiamo solo preoccuparci dell'esattezza a destra. Consideriamo dunque la successione esatta $M \xrightarrow{g} N \to 0$ (cioè g è surgettiva). Vorremmo che la successione trasformata $\mathrm{Hom}(P, M) \xrightarrow{g_*} \mathrm{Hom}(P, N) \to 0$ fosse esatta, cioè che g_* fosse surgettiva. Quindi, fissato $f \in \mathrm{Hom}(P, N)$, vogliamo trovare $\tilde{f} \in \mathrm{Hom}(P, M)$ tale che $f = g_*(\tilde{f}) = g \circ \tilde{f}$. In termini di diagrammi, abbiamo



Dunque P è proiettivo se e solo se, per ogni $g : M \longrightarrow N$ surgettiva e per ogni $f : P \longrightarrow N$, è possibile sollevare f a $\tilde{f} : P \longrightarrow M$ in modo che il diagramma di sopra commuti. In modo del tutto analogo, si può mostrare che E è iniettivo se e solo se, data $g : M \longrightarrow N$ iniettiva, e data $f : M \longrightarrow E$, esiste $\tilde{f} : N \longrightarrow E$ che estende f, in modo tale che commuti il seguente diagramma:[8]



Proposizione 3.11. Ogni modulo libero è proiettivo.

Dimostrazione. Sia $g : M \longrightarrow N$ surgettiva, e sia $f : F \longrightarrow N$, con F libero. Sia $\{e_i\}_i$ una base di F, e consideriamo le immagini $n_i = f(e_i)$. Poiché g è surgettiva, $\forall i\ \exists m_i \in M : g(m_i) = n_i$. Definiamo allora $\tilde{f} : F \longrightarrow M$, $\tilde{f}(e_i) = m_i$. Poiché $f(e_i) = g(\tilde{f}(e_i)) = n_i$, $f = g \circ \tilde{f}$ perché coincidono su una base di un modulo libero, da cui la tesi.

□

Con la prossima proposizione saremo in grado di dire in quali casi una successione esatta spezza.

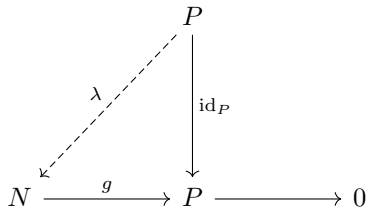
[8] Questo diagramma si ottiene prendendo quello per i moduli proiettivi e rovesciando tutte le frecce.

Proposizione 3.12 (Caratterizzazione dei moduli proiettivi)**.** Sia P un A-modulo. Allora sono equivalenti i seguenti fatti:

1. P è proiettivo;
2. $\mathrm{Hom}(P, \bullet)$ è un funtore esatto;
3. ogni successione esatta $0 \to M \to N \to P \to 0$ spezza;
4. P è addendo diretto di ogni modulo di cui è quoziente;
5. P è addendo diretto di un modulo libero.

Dimostrazione. ($1 \iff 2$) Già visto.

($1 \implies 3$) Dimostriamo che la successione spezza costruendo una sezione λ di g (cioè λ è tale che $g \circ \lambda = \mathrm{id}_P$), dove g è la mappa da N a P. Consideriamo il diagramma

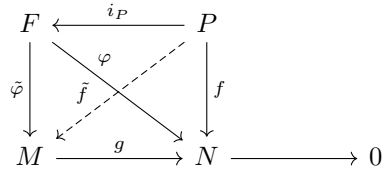


e osserviamo che, poiché P è proiettivo, l'identità di P si solleva a $\lambda : N \longrightarrow P$ tale che $g \circ \lambda = \mathrm{id}_P$.

($3 \implies 4$) Supponiamo che $P = N/M$. Allora abbiamo la successione esatta $0 \to M \to N \to P \to 0$, e per ipotesi la successione spezza, che è equivalente al fatto che $N \cong M \oplus P$. Dunque P è addendo diretto di N.

($4 \implies 5$) Sappiamo già che ogni modulo è quoziente di un modulo libero. Quindi, se $P = F/Q$, con F libero, $F \cong P \oplus Q$ e P è addendo diretto del modulo libero F.

($5 \implies 1$) Sia $F = P \oplus Q$, con F libero, e siano $g : M \longrightarrow N$ surgettiva, $f : P \longrightarrow N$. Se fissiamo un qualunque omomorfismo da Q a N (per esempio quello identicamente nullo), per la proprietà universale della somma diretta abbiamo una mappa $\varphi : F \longrightarrow N$ che commuta con le inclusioni; in particolare $\varphi \circ i_P = f$. Poiché F è libero, è anche proiettivo, dunque φ si solleva a $\tilde{\varphi} : F \longrightarrow M$ tale che $\varphi = g \circ \tilde{\varphi}$. Abbiamo il seguente diagramma:



e vogliamo definire $\tilde{f} : P \longrightarrow M$ tale che $f = g \circ \tilde{f}$. Se poniamo $\tilde{f} = \tilde{\varphi} \circ i_P$, si verifica che $g \circ \tilde{f} = g \circ \tilde{\varphi} \circ i_P = f$.

□

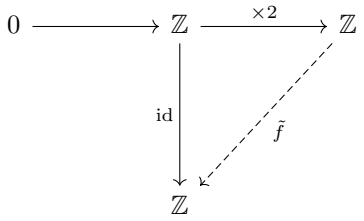
Osservazione. Nell'ultima implicazione abbiamo usato solo che F è proiettivo, quindi nella condizione 5 basta che P sia addendo diretto di un modulo proiettivo.

Si può verificare che vale un enunciato simile per i moduli iniettivi, cioè che per un A-modulo E sono fatti equivalenti:

1. E è iniettivo;
2. $\mathrm{Hom}(\bullet, E)$ è un funtore esatto;
3. ogni successione $0 \to E \to M \to N \to 0$ spezza;
4. se E è isomorfo a un sottomodulo di M, allora è un addendo diretto di M.

Mostriamo con un esempio che non sempre un sottomodulo di un modulo proiettivo è proiettivo. Sia $M = A = \mathbb{Z}/(4)$, e sia $N = (\overline{2})$. Ovviamente M è un A-modulo proiettivo (è libero). Mostriamo ora che N non è proiettivo. Se consideriamo $f : M \longrightarrow N,\ f(m) = \overline{2}m$, esso è un omomorfismo di A-moduli surgettivo, e il suo nucleo è $(\overline{2}) = N$. Per il primo teorema di isomorfismo $N = (\overline{2}) \cong (\mathbb{Z}/(4))/(\overline{2})$. Se N fosse proiettivo, allora $M = \mathbb{Z}/(4) \cong N \oplus N$, ma quest'ultimo isomorfismo è falso: per esempio, $\overline{2} \in \mathrm{Ann}(N \oplus N)$, ma $\overline{2} \notin \mathrm{Ann}(\mathbb{Z}/(4))$.

Abbiamo visto che i moduli liberi sono proiettivi, ma non è vero che i moduli liberi sono *iniettivi*. Per esempio, è ovvio che $\mathbb{Z}$ è uno $\mathbb{Z}$-modulo libero, ma se consideriamo il diagramma



una $\tilde{f}$ che faccia commutare il triangolo dovrebbe mandare 2 in 1, quindi $2\tilde{f}(1) = 1$, ma nessun intero moltiplicato per 2 dà 1. Dunque $\mathbb{Z}$ non è uno $\mathbb{Z}$-modulo iniettivo.

Non è neanche vero in generale che tutti i moduli proiettivi sono liberi. Sia $A = \mathbb{Z}[\sqrt{-6}]$, e sia $I = (2, \sqrt{-6})$, e facciamo vedere che I è un A-modulo proiettivo, ma non libero.

- I non è libero: osserviamo che, in generale, se I è un ideale di A non principale, allora non è un A-modulo libero: altrimenti, una base di I sarebbe un sistema di generatori, e conterrebbe almeno 2 elementi distinti non nulli a, b. Però $ab - ba = 0$, contraddicendo la libertà del sistema di generatori. Ci basta quindi mostrare che $I = (2, \sqrt{-6})$ non è principale: se $I = (a)$, a deve dividere 2 e $\sqrt{-6}$, che sono irriducibili (cosa che si può mostrare passando alle norme), dunque $a = 1$, ma $I \neq (1)$: infatti, $\mathbb{Z}[\sqrt{-6}]/(2, \sqrt{-6}) \cong \mathbb{Z}[x]/(x^2 + 6, 2, x) = \mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/(2) \neq 0$.

- I è proiettivo: sia $J = (3, \sqrt{-6})$. Notiamo che I e J sono comassimali $(1 = 3 - 2,\ 3 \in J,\ 2 \in I)$ e quindi $I \cap J = IJ$. Calcoliamo IJ: $IJ = (2, \sqrt{-6})(3, \sqrt{-6}) = (6, 2\sqrt{-6}, 3\sqrt{-6}, -6) = (\sqrt{-6})$. Dunque $I \cap J = IJ$ è un ideale principale. La mappa $g : \mathbb{Z}[\sqrt{-6}] \longrightarrow (\sqrt{-6}),\ 1 \mapsto \sqrt{-6}$ è surgettiva, e il suo nucleo è $\mathrm{Ann}(\sqrt{-6}) = 0$, essendo A un dominio (è un sottoanello di $\mathbb{C}$). Quindi $I \cap J \cong A$ è un A-modulo libero. Consideriamo adesso la mappa $f : I \oplus J \longrightarrow A,\ (i, j) \mapsto i + j$. f è un omomorfismo di A-moduli, è surgettivo, in quanto I e J sono comassimali, quindi $1 \in \mathrm{Im}\, f$, e $\ker f$ è dato da coppie $(i, -i)$ al variare di $i \in I$. La seconda coordinata è in J, perciò $i \in I \cap J$. Si ha dunque la successione esatta $0 \to I \cap J \to I \oplus J \to A \to 0$. In terza posizione compare A, che è un A-modulo proiettivo, quindi la successione spezza e $I \oplus J \cong (I \cap J) \oplus A \cong A \oplus A = A^2$. Allora I è addendo diretto del modulo libero A^2, e quindi proiettivo.

Vediamo un'ultima proprietà dei moduli proiettivi, alla quale premettiamo la seguente definizione:

Definizione (Modulo finitamente presentato)**.** Un A-modulo M si dice **finitamente presentato** se esiste una successione esatta $A^r \to A^n \to M \to 0$, con $r, n \in \mathbb{N}$.

Proposizione 3.13. Sia M un A-modulo proiettivo. Allora M è finitamente presentato se e solo se è finitamente generato.

Dimostrazione. ($\Longrightarrow$) Ovvio, e valido per tutti gli A-moduli (infatti, M è f.g. se esiste una mappa surgettiva da A^n a M, che è un pezzo della successione esatta nella definizione di finitamente presentato).

($\Longleftarrow$) Poiché M è finitamente generato, esiste $\psi : A^n \longrightarrow M$ surgettiva, dalla quale si ottiene la successione esatta $0 \to \ker\psi \to A^n \to M \to 0$. Essendo M proiettivo, si ha $A^n \cong \ker\psi \oplus M$. Vediamo ora che $\ker\psi$ è finitamente generato. In generale, sottomoduli di moduli f.g. non sono f.g., ma *addendi diretti* di moduli f.g. lo sono: infatti, se $M = N \oplus P$, la successione $0 \to N \to M \to P \to 0$ spezza, quindi c'è una retrazione $\eta : M \longrightarrow N$, che è surgettiva perché ha $i : N \hookrightarrow M$ come inversa destra. Si verifica facilmente che, se $m_1, ..., m_n$ generano M, allora $\eta(m_1), ..., \eta(m_n)$ generano N, che quindi è finitamente generato. Avendo provato che $\ker\psi$ è finitamente generato, prendiamo $\varphi : A^r \longrightarrow \ker\psi$ surgettiva. Allora, se i è l'inclusione di $\ker\psi$ dentro A^n, $i \circ \varphi : A^r \longrightarrow A^n$ è la funzione cercata. Dobbiamo verificare che la successione $A^r \xrightarrow{i\circ\varphi} A^n \xrightarrow{\psi} M$ è esatta, cioè che $\ker\psi = \mathrm{Im}(i \circ \varphi)$. Ma $\varphi(A^r) = \ker\psi$ in quanto φ è surgettiva, e ovviamente l'immagine di $\ker\psi$ tramite l'inclusione è $\ker\psi$, che conclude la dimostrazione.

□

3.7 Moduli su PID

Questa sezione è dedicata allo studio dei moduli su domini a ideali principali, che si scopriranno essere molto simili agli spazi vettoriali, e quindi molte tecniche

tipiche dell'algebra lineare possono essere applicate a questi oggetti. Vediamo una prima similitudine con gli spazi vettoriali.

Teorema 3.14. Sia A un PID, sia M un A-modulo libero finitamente generato[9], e sia N un sottomodulo non nullo di M. Allora anche N è libero, e $\operatorname{rank} N \leq \operatorname{rank} M$.

Dimostrazione. Procediamo per induzione su $r = \operatorname{rank} M$.

Passo base, $r = 1$: M è isomorfo ad A, e quindi N è isomorfo a un ideale di A diverso da 0. Poiché A è un PID, $N \cong (a)$, per qualche $a \in A \setminus \{0\}$. Allora $f : A \longrightarrow (a),\ 1 \mapsto a$ è un omomorfismo surgettivo, ed è iniettivo in quanto $a \neq 0$ e A è un dominio, quindi $N \cong (a) \cong A$, cioè N è libero di rango 1.

Passo induttivo, $r \implies r+1$: sia $\{m_1, ..., m_{r+1}\}$ una base di M, e poniamo $N_r = N \cap \langle m_1, ..., m_r \rangle$. N_r è un sottomodulo di $\langle m_1, ..., m_r \rangle$, che è libero di rango r, dunque per ipotesi induttiva N è libero, con $\operatorname{rank} N \leq r$. Se $N = N_r$, abbiamo concluso, quindi supponiamo che $N_r \subsetneq N$. Per ogni $n \in N$, esistono unici $b_1, ..., b_r, a_n \in A$ tali che $n = \sum_{i=1}^{r} b_i m_i + a_n m_{r+1}$. Poniamo $I = \{a_n \in A \mid n \in N\}$, e mostriamo che è un ideale di A. Ovviamente $0 \in I$ $(n = 0)$. Se $a_{n_1},\ a_{n_2} \in I$, presi $n_1 = \sum b_i m_i + a_{n_1} m_{r+1},\ n_2 = \sum c_i m_i + a_{n_2} m_{r+1}$, abbiamo $n_1 + n_2 = \sum (b_i + c_i) m_i + (a_{n_1} + a_{n_2}) m_{r+1}$, quindi $a_{n_1} + a_{n+2} \in I$. In modo simile si mostra che se $a_n \in I,\ r \in A$, allora $r a_n = a_{rn}$. Poiché A è un PID, $A = (a),\ a \in A$. Se $a = 0$, il coefficiente di m_{r+1} è nullo per ogni elemento di N, cioè $N \subseteq \langle m_1, ..., m_r \rangle$ e quindi $N = N_r$. Allora deve essere $a \neq 0$. Sia $n_0 \in N$ tale che $n_0 = \sum b_i m_i + a m_{r+1}$ (ovvero $a_{n_0} = a$). Per concludere, mostriamo che $N = N_r \oplus \langle n_0 \rangle$. In tal caso, N sarebbe libero (somma diretta di due liberi) di rango $1 + \operatorname{rank} N_r \leq r + 1$.

- $N_r \cap \langle n_0 \rangle = 0$: se $n \in N_r \cap \langle n_0 \rangle$, il coefficiente di m_{r+1} è nullo $(n \in N_r)$, ma $n = b n_0$, quindi il coefficiente di m_{r+1} è anche ab. Dunque $ab = 0$ e $a \neq 0$; essendo A un dominio, $b = 0$ e anche $n = 0$.
- $N \subseteq N_r + \langle n_0 \rangle$: sia $n \in N$, e scriviamo $n = \sum c_i m_i + h a m_{r+1}$. Allora $n - h n_0 = \sum (c_i - h b_i) m_i \in N_r$.

□

Corollario.
1. Se A è un PID, M un A-modulo finitamente generato e $N \subseteq M$, allora N è finitamente generato.
2. Se M è un A-modulo finitamente generato proiettivo, allora è libero.

Dimostrazione.
1. Sia $f : A^r \longrightarrow M$ surgettiva. Allora $f^{-1}(N)$ è un sottomodulo di A^r, quindi è libero di rango minore o uguale a $\operatorname{rank} A^r$; in particolare è finitamente generato. Se $m_1, ..., m_s$ generano $f^{-1}(N)$, allora $f(m_1), ..., f(m_s)$ generano N.

[9] Questo teorema vale anche se M non è finitamente generato, ma serve una dimostrazione diversa.

2. Se f è come nel punto precedente, allora abbiamo la successione esatta $0 \to \ker f \to A^r \to M \to 0$. M è proiettivo, quindi $A^r \cong \ker f \oplus M$. Quindi M è un addendo diretto di A^r, e in particolare un suo sottomodulo, quindi è libero per il teorema precedente.

□

Sia A un PID, e sia M un A-modulo finitamente generato. Se $\varphi : A^r \longrightarrow M$ è un omomorfismo surgettivo, il suo nucleo è un A-sottomodulo di A^r, dunque è libero, e isomorfo ad A^s per qualche $s \leq r$. Fissato un isomorfismo $\psi : A^s \longrightarrow \ker \varphi$, otteniamo la successione esatta $0 \to A^s \xrightarrow{i \circ \psi} A^r \to M \to 0$. Se poniamo $f = i \circ \psi$, allora $M \cong \operatorname{coker} f$. Ma f è una mappa A-lineare tra moduli liberi, quindi si rappresenta in modo unico con una matrice $X \in M_{r \times s}(A)$. Ovvero ogni A-modulo finitamente generato è conucleo di una matrice. Notiamo che c'è un'ambiguità su X dovuta alla scelta del numero di generatori r di M: tra poco Il nostro prossimo obiettivo è dimostrare che, con cambi di base opportuni in partenza e in arrivo, ogni matrice si può portare in forma diagonale.

Definizione. Una matrice $X \in M_{r \times s}(A)$ si dice **diagonale** se $X = (a_{ij})$ con $a_{ij} = 0$ se $i \neq j$.

Ricordiamo che le matrici trattate in questa sezione non sono necessariamente quadrate.

Definizione (Matrici equivalenti)**.** Due matrici $X, Y \in M_{r \times s}(A)$ si dicono **equivalenti** se $\exists R \in M_{r \times r}(A),\ S \in M_{s \times s}(A)$ invertibili tali che $Y = RXS$.

È facile verificare che l'equivalenza di matrici è una relazione di equivalenza. Le matrici R ed S corrispondono a un cambio di base in A^r e A^s rispettivamente.

ATTENZIONE: affinché una matrice $P \in M_{k \times k}(A)$ sia invertibile, non basta che abbia determinante diverso da 0: $\det(P)$ deve essere invertibile in A.

Un modo semplice di ottenere matrici equivalenti è effettuare *operazioni elementari* su righe e colonne. Ci sono due tipi di operazioni elementari:

- scambiare righe/colonne;
- sostituire a una riga/colonna a volte quella riga/colonna + b volte un'altra riga/colonna, con $a \in A^*,\ B \in A$.

La prima corrisponde a moltiplicare per una matrice di permutazione, che ha determinante ± 1, e la seconda è come moltiplicare per una matrice P della forma

$$P = \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & b & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \end{pmatrix}$$

che ha determinante $a \in A^*$. Dunque le matrici ottenute in questo modo sono davvero equivalenti. Queste operazioni sono analoghe a quelle per l'algoritmo di eliminazione gaussiana in algebra lineare.

Proposizione 3.15. Sia $X \in M_{r\times s}(A)$, e definiamo $\Delta_i(X)$ come l'ideale generato dai determinanti dei minori $i \times i$ di X. Se X e Y sono equivalenti, allora $\forall 1 \leq s\ \Delta_i(X) = \Delta_i(Y)$.

Dimostrazione. L'osservazione cruciale è che, se $R \in M_{r\times r}(A)$, allora vale che $\Delta_i(RX) \subseteq \Delta_i(X)$. Infatti, poiché ogni entrata di RX è combinazione lineare delle entrate di X, tutti i minori $i \times i$ di RX sono combinazioni lineari di minori $i\times i$ di X. Per la multilinearità del determinante, anche i determinanti dei minori $i \times i$ di RX, che generano $\Delta_i(RX)$, sono combinazioni lineari di determinanti di minori $i \times i$ di X, ovvero dei generatori di $\Delta_i(X)$. Quindi $\Delta_i(RX) \subseteq \Delta_i(X)$. Se ora supponiamo R invertibile, abbiamo $\Delta_i(X) = \Delta_i(R^{-1}RX) \subseteq \Delta_i(RX) \subseteq \Delta_i(X)$. Dunque tutti i contenimenti sono uguaglianze, in particolare $\Delta_i(RX) = \Delta_i(X)$. Se invece $S \in M_{s\times s}(A)^*$, basta osservare che a ogni minore $i \times i$ di XS corrisponde un minore $i \times i$ di $(XS)^T$ con lo stesso determinante, dunque $\Delta_i(XS) = \Delta_i((XS)^T) = \Delta_i(S^TX^T) = \Delta_i(X^T) = \Delta_i(X)$. Quindi $\Delta_i(X) = \Delta_i(RXS) = \Delta_i(Y)$.

□

Descriviamo ora un algoritmo per ridurre ogni matrice X a una matrice diagonale equivalente.

Teorema 3.16. Ogni matrice $X \in M_{r\times s}(A)$ è equivalente a una matrice diagonale.

Dimostrazione. Partiamo dal caso 2×2. Sia $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, con a, c non entrambi nulli. Sia $\alpha = \gcd(a, c)$. Sfruttando l'identità di Bézout, scriviamo $\alpha = xa + yc$. Allora la matrice $R = \begin{pmatrix} x & y \\ -c/\alpha & a/\alpha \end{pmatrix}$ ha determinante 1 (dunque è invertibile), e tale che

$$RX = \begin{pmatrix} x & y \\ -c/\alpha & a/\alpha \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}.$$

Vogliamo ora azzerare l'entrata in cui si trova β. Poniamo $\delta = \gcd(\alpha, \beta)$, scriviamo $\delta = u\alpha + v\beta$, e moltiplichiamo RX a destra per $S = \begin{pmatrix} u & -\beta/\delta \\ v & \alpha/\delta \end{pmatrix}$. Si ottiene una matrice triangolare superiore, ma l'entrata in basso a destra potrebbe essere di nuovo non nulla. Ripetiamo il procedimento, applicandolo una volta alla prima riga, una volta alla prima colonna, finché la matrice non è in forma diagonale. Dimostriamo che prima o poi questo procedimento termina. Se chiamiamo α_i l'elemento di posto (1,1) dopo i passi ($\alpha_0 = a$), notiamo che $\alpha_{i+1}|\alpha_i$, poiché α_{i+1} si ottiene facendo il massimo comun divisore tra α_i e qualcos'altro. Si ha quindi una catena ascendente di ideali $(\alpha_0) \subseteq (\alpha_1) \subseteq \cdots$, che deve stabilizzarsi in quanto A è un PID. Sia (λ) l'elemento massimale della catena; allora λ deve

dividere sia l'elemento di posto (1,2) che quello di posto (2,1), cioè la matrice X si è ridotta a $\begin{pmatrix} \lambda & r\lambda \\ s\lambda & * \end{pmatrix}$. Sottraendo alla seconda riga s volte la prima, e alla seconda colonna r volte la prima, si ottiene $\begin{pmatrix} \lambda & 0 \\ 0 & * \end{pmatrix}$, che è diagonale.

Passiamo ora al caso generale. Se $X = 0$, abbiamo finito. Altrimenti, con scambi di righe e colonne possiamo portare un'entrata non nulla di X al posto (1,1). Concentriamoci ora sul blocco 2×2 di X in alto a sinistra, della forma $X' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Dal caso trattato sopra, esistono R', S' tali che $R'X'S'$ è diagonale. Se R, S sono diagonali a blocchi, con un blocco 2×2 uguale a R' (o S'), e l'altro blocco uguale all'identità, allora RXS diagonalizza il blocco in alto a sinistra di X. Adesso ripetiamo il procedimento: portiamo un elemento non nullo della prima colonna al posto (2,1) e diagonalizziamo il blocco in alto, finché tutta la prima colonna non è della forma $(d, 0, ..., 0)^T$. A questo punto facciamo lo stesso con la prima riga, portando gli elementi non nulli della riga al posto (1,2) e diagonalizzando finché la prima riga non è tutta nulla, a meno dell'elemento sulla diagonale. Potrebbero esserci dei nuovi elementi non nulli nella prima colonna, quindi ripetiamo il tutto sulla prima colonna, e poi sulla prima riga, finché la prima colonna e la prima riga sono entrambe nulle (tranne, possibilmente, l'elemento sulla diagonale). Come nel caso 2×2, questo avviene in un numero finito di passi, poiché, se α_i è l'elemento di posto (1,1) al passo i, α_{i+1} divide α_i, e la catena di divisibilità è stazionaria essendo A un PID. Se l'ultimo elemento della catena è λ, a questo punto λ divide tutti gli elementi della prima riga e della prima colonna. quindi sottraendo alle altre righe/colonne opportuni multipli della prima riga/colonna azzeriamo tutti gli elementi non diagonali della prima riga/colonna. Ora, ripetiamo tutto sulla sottomatrice ottenuta "ignorando" la prima riga e la prima colonna, che è più piccola, e iterando il procedimento si arriva alla forma diagonale.

□

In pratica, questo algoritmo non è molto utile, perché può richiedere molto tempo e molti calcoli. Quindi è meglio ridurre prima X tramite operazioni elementari per ottenere quanti più zeri possibile, e poi applicare l'algoritmo. A breve vedremo una scorciatoia che sfrutta gli invarianti $\Delta_i(X)$.

Definizione (Forma normale di Smith)**.** Una matrice $X \in M_{r\times s}(A)$ è in **forma normale di Smith** se è diagonale e, se $d_1, ..., d_s$ sono gli elementi diagonali, con d_i al posto (i, i), allora $d_1|d_2| \cdots |d_s$.

Teorema 3.17. Ogni matrice X è equivalente a una matrice in forma di Smith.

Dimostrazione. Per il teorema precedente, X è equivalente a una matrice diagonale, quindi possiamo supporre che X sia diagonale, con elementi diagonali $d_1, ..., d_s$. Se X non è in forma di Smith, esistono i, j con $i < j$ tali che $d_i \nmid d_j$. Prendiamo i minimo con questa proprietà, e j tale che $d_i \nmid d_j$. Tramite scambi di righe e colonne possiamo portare d_i, d_j in alto a sinistra. Se $\tilde{d}_i = \gcd(d_i, d_j)$,

possiamo scrivere $\tilde{d_i} = \alpha d_i + \beta d_j$ per certi $\alpha, \beta \in A$. Allora, moltiplicando $\begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix}$ a sinistra per $\begin{pmatrix} \alpha & \beta \\ -d_j/\tilde{d_i} & d_i/\tilde{d_i} \end{pmatrix}$ e a destra per $\begin{pmatrix} 1 & -\beta d_j/\tilde{d_i} \\ 1 & \alpha d_j \tilde{d_i} \end{pmatrix}$, si ottiene $\begin{pmatrix} \tilde{d_i} & 0 \\ 0 & d_i d_j/\tilde{d_i} \end{pmatrix}$. Osserviamo che $\tilde{d_i}$ divide sia d_i che d_j, e quindi divide anche $\tilde{d_j} = d_i d_j/\tilde{d_i}$. Inoltre, per la minimalità dell'indice i, $\forall k < i$ $d_k | d_i$ e $d_k | d_j$, quindi $d_k | \gcd(d_i, d_j) = \tilde{d_i}$. Riportando $\tilde{d_i}, \tilde{d_j}$ alle righe i, j rispettivamente, ora $\tilde{d_i} | \tilde{d_j}$. Possiamo ripetere il procedimento appena descritto finché il "nuovo" d_i ottenuto (che non è necessariamente uguale a $\tilde{d_i}$) non divide tutti i successivi d_k. Iterando la procedura, si arriva alla forma di Smith.

□

Illustriamo con un esempio una "scorciatoia" per giungere alla forma normale di Smith, sfruttando i Δ_i.

Esempio. *Sia* $X = \begin{pmatrix} 6 & 0 & 2 \\ 4 & 8 & 2 \\ 4 & 4 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{Z})$. *La forma di Smith di* X *sarà* $S = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$, *con* $a|b|c$. *Per l'invarianza dei* Δ_i *abbiamo che* $\Delta_1(X)$ *è generato dai singoli elementi di* S, *dunque dal loro massimo comun divisore, che è a per le relazioni di divisibilità.* $\Delta_2(X)$ *è generato dai determinanti dei minori* 2×2, *che sono* 0 *o prodotti di elementi diagonali. Il loro massimo comun divisore è* ab, *ovvero* $\Delta_2(X) = (a)(b) = (b)\Delta_1(X)$. *Invece* $\Delta_3(X)$ *è generato da* $\det(S) = abc$, *cioè* $\Delta_3(X) = (ab)(c) = (c)\Delta_2(X)$. *Questo è valido in generale: per ogni* $1 \leq i \leq s-1$, $\Delta_{i+1}(X) = (d_{i+1})\Delta_i(X)$, *dove* $d_1, ..., d_s$ *sono gli elementi diagonali della forma di Smith di* X. *Tornando all'esempio, possiamo calcolare i* Δ_i *direttamente da* X*:* $\Delta_1(X)$ *è generato dal massimo comun divisore delle entrate di* X, *che è* 2; *quindi* $\Delta_1(X) = (a) = 2$, *ovvero* $a = \pm 2$. *Osserviamo che* a, b, c *sono definiti a meno di invertibili; poniamo* $a = 2$. $\Delta_2(X)$ *richiede di calcolare il determinante di 9 minori di* X, *che è un po' laborioso, ma per* $\Delta_3(X)$ *basta il determinante di* X, *che è* 16. *Dunque abbiamo* $a = 2$, $abc = 16$, $a|b|c \implies bc = 8$, $2|b|c$. *L'unica possibilità è* $b = 2$, $c = 4$, *dunque la forma di Smith di* X *è* $S = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$.

Anche nel caso generale gli elementi diagonali della forma di Smith sono definiti a meno di invertibili, ma vedremo che non sarà un problema grave. Tutto il lavoro appena svolto sulla diagonalizzazione ci permette di dimostrare il prossimo risultato:

Teorema 3.18. Sia A un PID, M un A-modulo finitamente generato libero e sia N un sottomodulo di M. Allora esistono $\{m_1, ..., m_r\}$ base di M e $d_1|d_2|\cdots|d_s \in A$ tali che $\{d_1 m_1, ..., d_s m_s\}$ è una base di N.

Dimostrazione. Fissiamo una base $\{\tilde{m_1}, ..., \tilde{m_r}\}$ di M. Sappiamo che anche N è libero di rango $s \leq r$: sia $\{n_1, ..., n_s\}$ una base di N. Allora $\exists X \in M_{r\times s}(A) : (\tilde{m_1}, ..., \tilde{m_r})X = (n_1, ..., n_s)$. Portiamo X in forma normale di Smith: siano $R \in M_{r\times r}(A)^*,\ S \in M_{s\times s}(A)^*$ tali che $RXS = D$, con D in forma di Smith: siano inoltre $d_1, ..., d_s$ gli elementi diagonali di D: per definizione di forma di Smith $d_1|d_2|\cdots|d_s$. $(\tilde{m_1}, ..., \tilde{m_r})R^{-1} = (m_1, ..., m_r)$ è ancora una base di M, e abbiamo $(\tilde{m_1}, ..., \tilde{m_r})R^{-1}RXS = (n_1, ..., n_s)S$, che è ancora una base di N. D'altro canto $(\tilde{m_1}, ..., \tilde{m_r})R^{-1}RXS = (m_1, ..., m_r)D = (d_1m_1, ..., d_sm_s)$, in quanto D è diagonale. Quindi $\{d_1m_1, ..., d_sm_s\}$ è una base di N, e in particolare i d_i sono tutti non nulli.

□

Siamo giunti all'obiettivo finale, che descrive la struttura di un modulo finitamente generato su un PID:

Teorema 3.19 (Teorema di struttura per moduli finitamente generati su PID)**.** Sia M un A-modulo finitamente generato, con A un PID. Allora $\exists d_1|\cdots|d_s$ non nulli, univocamente determinati da M, tali che $M \cong \bigoplus_{i=1}^{s} A/(d_i) \oplus A^{r-s}$. Il pezzo A^{r-s} si dice **parte libera**, l'altro pezzo è la **parte di torsione**.

Dimostrazione. Sia $f : A^r \longrightarrow M$ surgettiva. Applichiamo il teorema precedente ad A^r e a $\ker f$: abbiamo quindi $\{m_1, ..., m_r\}$ base di A^r e $d_1|\cdots|d_s$ non nulli tali che $\{d_1m_1, ..., d_sm_s\}$ è una base di $\ker f$. Se i è l'inclusione di $\ker f$ dentro A^r, allora $M \cong \operatorname{coker} i = A^r/\ker f$. Essendo $\ker f = \bigoplus_{i=1}^{s}(d_i)m_i$, abbiamo $M \cong (\bigoplus_{i=1}^{r} Am_i)/\ker f \cong \bigoplus_{i=1}^{s} Am_i/(d_i)m_i \oplus A^{r-s} \cong \bigoplus_{i=1}^{s} A/(d_i) \oplus A^{r-s}$.

Per dimostrare l'unicità, ci serviremo di questo fatto: se A è un anello e $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r,\ J_1 \supseteq J_2 \supseteq \cdots \supseteq J_{r_1}$ sono due catene di ideali tali che $\bigoplus_{i=1}^{r} A/I_i \cong \bigoplus_{i=1}^{r_1} A/J_i$, con $r_1 \geq r$, allora:

1. $J_i = (1)\ \forall 1 \leq j \leq r_i - r$;
2. $J_{r_1-r+i} = I_i\ \forall 1 \leq j \leq r$.

Questo implica l'unicità della scrittura perché, scegliendo due insiemi diversi di generatori per M, allora $M \cong \bigoplus_{i=1}^{r} A/(d_i) \cong \bigoplus_{i=1}^{r_1} A/(d'_i)$ (con alcuni d_i, d'_i possibilmente nulli), e la condizione sui d_i fa sì che $(d_1) \supseteq \cdots \supseteq (d_r)$, $(d'_1) \supseteq \cdots \supseteq (d'_{r_1})$. Dunque $(d'_1) = \cdots = (d_{r_1-r}) = (1)$, ossia i primi $r_1 - r$ addendi diretti sono 0, e $A/(d'_{r_1-r+i}) = A/(d_i)$. Dimostriamo il fatto appena enunciato:

1. Poiché $M \cong \bigoplus_{i=1}^{r} A/I_i \cong \bigoplus_{i=1}^{r_1} A/J_i$, si ha che $M/J_1M \cong \bigoplus_{i=1}^{r} A/(I_i + J_1) \cong \bigoplus_{i=1}^{r_1} A/(J_1 + J_i) = (A/J_1)^{r_1}$, in quanto J_1 contiene tutti i J_i. Dalla prima scrittura di M/J_1M si deduce che M/J_1M è quoziente di $(A/J_1)^r$, e per la

seconda scrittura abbiamo una mappa surgettiva da $(A/J_1)^r$ in $(A/J_1)^{r_1}$, che implica $r \geq r_1$. Poiché per ipotesi $r_1 \geq r$, o $r = r_1$, o $A/J_1 = 0$, ovvero $J_1 = (1)$. Possiamo ripetere questo ragionamento per affermare che $J_1 = \cdots = J_{r_1 - r}$.

2. Per il punto precedente possiamo supporre $r_1 = r$. Sia $a \in I_1$, e consideriamo aM. Abbiamo che $aM \cong \bigoplus_{i=1}^{r} aA/I_i \cong \bigoplus_{i=1}^{r} A/(I_i : a)$: infatti, la mappa $A \to A/I_i \xrightarrow{\times a} aA/I_i$ è surgettiva, e il suo nucleo sono gli elementi che moltiplicati per a finiscono in I_i, cioè proprio $I_i : a$. Allo stesso modo, $aM \cong \bigoplus_{i=1}^{r} A/(J_i : a)$. Ma $a \in I_1$, quindi $I_1 : a = (1)$. Inoltre per ogni i $I_i : a \supseteq I_{i+1} : a,\ J_i : a \supseteq J_{i+1} : a$, quindi per il punto 1 $J_1 : a = (1)$, ovvero $a \in J_1$. Abbiamo allora $I_1 \subseteq J_1$, e simmetricamente $J_1 \subseteq I_1$. Ripetendo il ragionamento per gli altri I_i, J_i si ha la tesi.

□

Questo teorema è una generalizzazione del teorema di struttura per gruppi abeliani finiti (o anche finitamente generati): basta prendere $A = \mathbb{Z}$.

Osservazione. Alla luce del teorema di struttura è possibile risolvere l'ambiguità legata al numero di generatori di M: poiché il rango della parte libera di M dipende solo da M, se avessimo scelto $r+h$ generatori per M, otterremmo $s+h$ termini nella parte libera da torsione. Ma anche i d_i dipendono unicamente da M, quindi si avrebbe che $A/(d_j) = 0$ per ogni $j \leq h$, cioè $d_1, ..., d_h \in A^*$. In un esempio concreto, una volta descritto M come conucleo di una matrice X, se nella forma di Smith di X compaiono degli invertibili, allora il numero dei generatori di M scelti all'inizio non era minimale.

Di solito, per i gruppi abeliani finiti si usa la scomposizione nei suoi p-Sylow, quindi vorremmo un analogo di tale scomposizione per moduli finitamente generati.

Definizione (Sottomodulo di torsione)**.** Sia A un dominio ed M un A-modulo. Il **sottomodulo di torsione** di M è $T(M) = \{m \in A \mid \exists a \in A \setminus \{0\} : am = 0\}$.

$T(M)$ è un sottomodulo di M: infatti, $0 \in M$ $(1 \cdot 0 = 0)$; se $m, n \in T(M)$ e $a, b \in A \setminus \{0\}$ sono tali che $am = bn = 0$, allora $ab(m+n) = 0$, e $ab \neq 0$ poiché A è un dominio; se $m \in T(M)$ con $am = 0,\ a(bm) = 0\ \forall b \in A$.

Dato $a \in A$, definiamo la *a-componente* di M come

$$M_{[a]} = \{m \in T(M) \mid \exists k \in \mathbb{N} : a^k m = 0\}.$$

La condizione $a^k m = 0$ per qualche k è equivalente a richiedere che $(a) \subseteq \sqrt{\mathrm{Ann}(m)}$.

Supponiamo che A sia un PID, ed M un A-modulo finitamente generato. Sappiamo che $M \cong \bigoplus_{i=1}^{s} A/(d_i) \oplus A^{r-s}$, con i d_i non nulli, e $d_1 | \cdots | d_s$.

Ciascun d_j si fattorizza in irriducibili (A è anche un UFD): $(d_j) = \prod_{i=1}^{t_j} (\pi_{ij}^{e_{ij}})$. Ricordiamo che in un PID gli elementi irriducibili generano ideali massimali; inoltre, se π_1, π_2 sono irriducibili distinti, $\pi_1^{e_1}, \pi_2^{e_2}$ sono elementi coprimi, e per Bézout $(\pi_1^{e_1})$ e $(\pi_2^{e_2})$ sono comassimali. Perciò $(d_j) = \bigcap_{i=1}^{t_j} (\pi_{ij}^{e_{ij}})$, e applicando il teorema cinese del resto ad $A/(d_j)$ si ottiene $A/(d_j) \cong \bigoplus_{i=1}^{t_j} A/(\pi_{ij}^{e_{ij}})$ Se $p_1, ..., p_k$ sono i primi che compaiono nella fattorizzazione di d_s (e quindi degli altri d_j), possiamo riordinare gli addendi diretti che costituiscono $T(M)$, ottenendo $T(M) \cong \bigoplus_{j=1}^{s} A/(d_j) = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{s} A/(p_i^{e_{ij}})$. Ciascun termine $\bigoplus_{j=1}^{s} A/(p_i^{e_{ij}})$ ha come annullatore una potenza di p_i, quindi è la p_i-componente di $T(M)$, e possiamo scrivere $T(M) \cong \bigoplus_{j=1}^{s} M_{[p_i]}$, che è l'analogo della decomposizione in p-Sylow di un gruppo abeliano finito.

4 Prodotto tensoriale e moduli piatti

Introduciamo una nuova operazione tra A-moduli: il prodotto tensoriale, che dati due moduli M, N, "trasforma" mappe bilineari da $M \times N$ in mappe lineari dal loro prodotto tensoriale. Poi lo studieremo come funtore, e definiremo la classe dei moduli piatti.

4.1 Prodotto tensoriale

Iniziamo definendo le applicazioni bilineari, che svolgono un ruolo centrale nella costruzione del prodotto tensoriale:

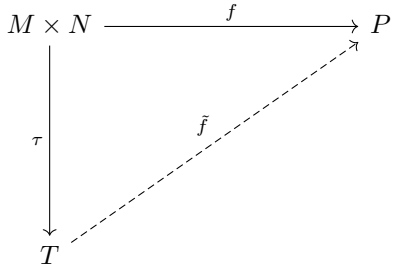
Definizione. Siano M, N, P tre A-moduli. $f : M \times N \longrightarrow P$ si dice **bilineare** se $\forall m_0 \in M,\ n_0 \in N\ f(m_0, \cdot) : N \longrightarrow P$ e $f(\cdot, n_0) : M \longrightarrow P$ sono A-lineari.

Denotiamo con $\mathrm{Bil}(M, N; P)$ l'insieme delle applicazioni bilineari da $M \times N$ in P.

Possiamo dotare $\mathrm{Bil}(M, N; P)$ di una somma e di un prodotto per scalari nel seguente modo: $\forall f, g \in \mathrm{Bil}(M, N; P),\ a \in A\ (f + g)(m, n) = f(m + n) + g(m, n);\ (af)(m, n) = af(m, n)$. Si verifica facilmente che tali operazioni definiscono una struttura di A-modulo su $\mathrm{Bil}(M, N; P)$.

Osserviamo che $\mathrm{Bil}(M, N; P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P))$. Infatti, data $b \in \mathrm{Bil}(M, N; P)$, definiamo $\varphi_b : M \longrightarrow \mathrm{Hom}(N, P)$ in questo modo: $\varphi_b(m) : N \longrightarrow P,\ (\varphi_b(m))(n) = b(m, n)$. Viceversa, se $\varphi : M \longrightarrow \mathrm{Hom}(N, P)$, possiamo definire $b_\varphi : M \times N \longrightarrow P,\ b_\varphi(m, n) = (\varphi(m))(n)$. Ci sono diverse cose da verificare: buona definizione delle mappe (ovvero φ_b è lineare e b_φ è bilineare), linearità di $b \mapsto \varphi_b$ e $\varphi \mapsto b_\varphi$, e il fatto che siano una l'inversa dell'altra.

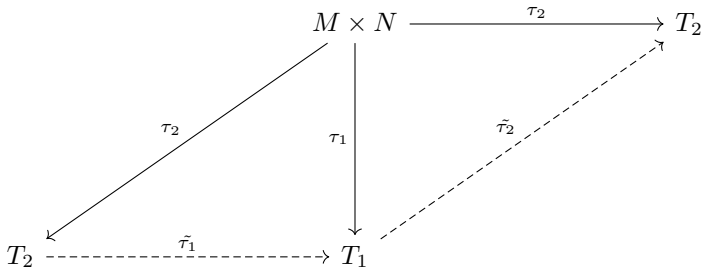
Definizione (Prodotto tensoriale)**.** Sia A un anello ed M, N A-moduli. Un **prodotto tensoriale** di M ed N è una coppia (T, τ), con T un A-modulo e $\tau : M \times N \longrightarrow T$ bilineare, tale che per ogni A-modulo P e per ogni $f \in \mathrm{Bil}(M, N; P)$ $\exists! \tilde{f} : T \longrightarrow P$ *lineare* che fa commutare il diagramma



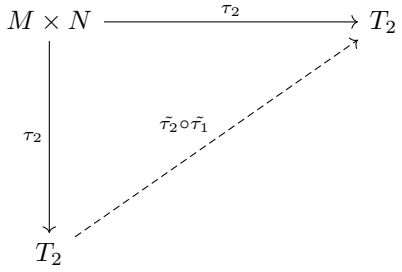
La proprietà soddisfatta da T è detta *proprietà universale* del prodotto tensoriale.

Teorema 4.1. Se M, N sono due A-moduli, un prodotto tensoriale esiste ed è unico a meno di isomorfismo.

Dimostrazione. Unicità: siano (T_1, τ_1), (T_2, τ_2) due prodotti tensoriali di M, N. Sfruttando la proprietà universale sia di T_1 che di T_2, otteniamo il diagramma commutativo

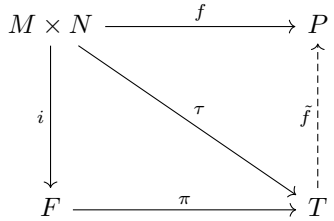


Quindi $\tilde{\tau_2} \circ \tilde{\tau_1}$ fa commutare il diagramma



Poiché anche l'identità di T_2 fa commutare tale diagramma, per unicità del sollevamento abbiamo $\tilde{\tau_2} \circ \tilde{\tau_1} = \mathrm{id}_{T_2}$ .Analogamente si ottiene che $\tilde{\tau_1} \circ \tilde{\tau_2} = \mathrm{id}_{T_1}$,quindi T_1 e T_2 sono isomorfi.

Esistenza: sia F il modulo libero $A^{M\times N}$, sia $i : M \times N \longrightarrow F$, $(m, n) \mapsto e_{m,n}$ (elementi della base canonica di $A^{M\times N}$). i è solo una funzione di insiemi, e vogliamo imporre la bilinearità di i, quindi quozientiamo F per un certo sottomodulo D al fine di introdurre le relazioni di bilinearità. Dunque $D = \langle i(m + m', n) - i(m, n) - i(m', n),\ i(am, n) - ai(m, n),\ i(m, n + n') - i(m, n) - i(m, n'),\ i(m, an) - ai(m, n) \mid m, m' \in M,\ n, n' \in N,\ a \in A\rangle_A$. Se π è la proiezione da F a $T = F/D$, abbiamo che $\tau = \pi \circ i : M \times N \longrightarrow T$ è bilineare per costruzione. Resta da verificare che (T, τ) soddisfa la proprietà universale. Sia P un A-modulo e fissiamo $f : M \times N \longrightarrow P$ bilineare. Vogliamo costruire $\tilde{f} : T \longrightarrow P$ tale che $\tilde{f} \circ \tau = f$. La situazione è descritta dal seguente diagramma:



Sia $\varphi : F \longrightarrow P,\ \varphi(e_{m,n}) = f(m,n)$, estesa per linearità a tutto F. In particolare $\varphi(i(m,n)) = \varphi(e_{m,n}) = f(m,n)$, cioè $\varphi \circ i = f$. Definiamo $\tilde{f} : T \longrightarrow P,\ \tilde{f}(\overline{x}) = \varphi(x)$. Verifichiamo che $\tilde{f}$ sia ben definita: ciò equivale a mostrare che $\varphi(d) = 0\ \forall d \in D$. I generatori di D sono di 4 tipi: uno, per esempio, è $d = i(m+m',n) - i(m,n) - i(m',n)$. Abbiamo che $\varphi(d) = f(m+m',n) - f(m,n) - f(m,n) = 0$ per la bilinearità di f. Lo stesso ragionamento funziona per gli altri tipi di generatori, concludendo la verifica. Mostriamo ora che $\tilde{f}$ fa commutare il diagramma, cioè $\tilde{f} \circ \tau = f$: sapendo che $\tau = \pi \circ i,\ \tilde{f}(\tau(m,n)) = \tilde{f}(\pi(i(m,n))) = \tilde{f}(\pi(e_{m,n})) = \tilde{f}(\overline{e_{m,n}}) = \varphi(e_{m,n}) = f(m,n)$, come voluto. Infine facciamo vedere che $\tilde{f}$ è unica. Se $\tilde{f}_1,\ \tilde{f}_2$ sono due sollevamenti di f, allora $\tilde{f}_1 \circ \tau = f = \tilde{f}_2 \circ \tau \implies \tilde{f}_1(\pi(i(m,n))) = \tilde{f}_1(\pi(e_{m,n})) = \tilde{f}_2(\pi(e_{m,n})) = \tilde{f}_2(\pi(i(m,n)))$. Allora $\tilde{f}_1 \circ \pi$ e $\tilde{f}_2 \circ \pi$ coincidono su una base di F, dunque sono uguali. Preso $x \in T$, per la surgettività di $\pi\ \exists y \in F : \pi(y) = x$, e quindi $\tilde{f}_1(x)) = \tilde{f}_1(\pi(y)) = \tilde{f}_2(\pi(y)) = \tilde{f}_2(x)$.

□

In pratica questa costruzione è inutile, se non per questa dimostrazione, e si usa invece la proprietà universale.

Da adesso il prodotto tensoriale di M ed N sarà denotato con $M \otimes_A N$, e $\tau(m,n) = m \otimes n$. Gli elementi di $M \otimes N$ sono detti *tensori*, e quelli della forma $m \otimes n$ con $m \in M,\ n \in N$ sono i *tensori elementari*.

Dalla bilinearità di τ si ha, per ogni $m, m' \in M,\ n, n' \in N,\ a \in A,\ (m + m') \otimes n = m \otimes n + m' \otimes n,\ m \otimes (n + n') = m \otimes n + m \otimes n',\ (am) \otimes n = a(m \otimes n) = m \otimes (an)$. Un'altra proprietà immediata è che $m \otimes 0 = 0$: infatti, $m \otimes 0 = m \otimes (0 + 0) = m \otimes 0 + m \otimes 0 \implies m \otimes 0 = 0$. Allo stesso modo si ha $0 \otimes n = 0$.

Proposizione 4.2. Sia G_1 un insieme di generatori di M e G_2 un insieme di generatori di N. Allora $G_1 \otimes G_2 = \{g_1 \otimes g_2 \mid g_1 \in G_1,\ g_2 \in G_2\}$ è un insieme di generatori per $M \otimes N$.

Dimostrazione. Sia L il sottomodulo generato da $G_1 \otimes G_2$. Mostriamo che $(M \otimes N)/L = 0$, che equivale a $L = M \otimes N$. La mappa identicamente nulla da $M \times N$ a $(M \otimes N)/L$ è bilineare, e per la proprietà universale induce una mappa lineare da $M \otimes N$ a $(M \otimes N)/L$. Ovviamente la mappa nulla fa commutare il diagramma. Mostriamo che anche $\pi : M \otimes N \longrightarrow (M \otimes N)/L$ lo fa commutare; dall'unicità del sollevamento seguirà $\pi = 0$, e quindi la tesi. Siano $m \in M,\ n \in N$, e scriviamo $m = \sum a_i m_i,\ n = \sum b_j n_j$, con $a_i, b_j \in A,\ m_i \in G_1,\ n_j \in G_2$. Si ha $\pi(\tau(m,n)) = \pi(m \otimes n) = \pi(\sum a_i m_i \otimes \sum b_j n_j) = \sum a_i b_j \pi(m_i \otimes n_j) = 0$, in quanto $m_i \otimes n_j \in G_1 \otimes G_2 \subseteq L$.

□

Prendendo $G_1 = M,\ G_2 = N$ si ottiene che i tensori elementari generano $M \otimes N$.

Vediamo alcune proprietà utili per calcolare i prodotti tensoriali:

Proposizione 4.3 (Proprietà del prodotto tensoriale)**.** Sia A un anello, M, N, P degli A-moduli, e I un ideale di A.

1. $A \otimes M \cong M$;
2. $M \otimes N \cong N \otimes M$;
3. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$;
4. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$;
5. $A/I \otimes M \cong M/IM$;
6. se M, N sono liberi di rango m, n rispettivamente, allora $M \otimes N$ è libero di rango mn.

Dimostrazione. Dimostriamo 1, 2, 6.

1. La mappa $f : A \times M \longrightarrow M,\ f(a, m) = am$ è bilineare, e definisce $\tilde{f} : A \otimes M \longrightarrow M,\ \tilde{f}(a \otimes m) = am$. Abbiamo anche l'applicazione lineare $g : M \longrightarrow A \otimes M,\ m \mapsto 1 \otimes m$. Inoltre $\tilde{f}(g(m)) = \tilde{f}(1 \otimes m) = m,\ g(\tilde{f}(a \otimes m)) = g(am) = 1 \otimes (am) = a \otimes m$, quindi g ed $\tilde{f}$ sono inverse, e danno l'isomorfismo cercato.

2. $f : M \times N \longrightarrow N \otimes M,\ (m, n) \mapsto n \otimes m$ e $g : N \times M \longrightarrow M \otimes N,\ (n, m) \mapsto m \otimes n$ sono bilineari, e inducono $\tilde{f}(m \otimes n) = n \otimes m,\ \tilde{g}(n \otimes m) = m \otimes n$, che sono chiaramente una l'inversa dell'altra, fornendo l'isomorfismo voluto.

6. Siano $M = A^m$. $N = A^n$, e procediamo per induzione su n. Se $n = 1$, abbiamo $A^m \otimes A \cong A^m$. Se assumiamo la tesi per $n - 1$, allora $A^m \otimes A^n \cong A^m \otimes (A^{n-1} \oplus A) \cong (A^m \otimes A^{n-1}) \oplus (A^m \otimes A) \cong A^{m(n-1)} \oplus A^m \cong A^{mn}$.

□

Vediamo alcuni esempi di calcolo del prodotto tensoriale:

- $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Q}$, per la proprietà 1.
- Dimostriamo che $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. Definiamo $f : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q},\ (a, b) \mapsto ab$. f è bilineare, e induce $\tilde{f} : \mathbb{Q} \otimes \mathbb{Q} \longrightarrow \mathbb{Q},\ a \otimes b \mapsto ab$. Poiché f è surgettiva ($a = f(1, a)$), abbiamo $a = \tilde{f}(1 \otimes a)$ e anche $\tilde{f}$ è surgettiva. Inoltre, essendo $\mathbb{Q}$ un dominio, $\tilde{f}(a \otimes b) = 0$ se e solo se $a = 0$ o $b = 0$, cioè $a \otimes b = 0$. Quindi 0 è l'unico tensore *elementare* che viene mandato in 0. Questo NON implica l'iniettività di $\tilde{f}$! Potrebbero ancora esserci dei tensori non elementari che hanno immagine 0. In questo caso particolare, però, tutti i tensori sono elementari. Innanzitutto, osserviamo che, se $m, n \in \mathbb{Q}$, con $n = \frac{a}{b},\ a, b \in \mathbb{Z}$, allora $m \otimes n = m \otimes \frac{a}{b} = b\frac{m}{b} \otimes \frac{a}{b} = a\frac{m}{b} \otimes \frac{b}{b} = m\frac{a}{b} \otimes 1 = mn \otimes 1$. Se ora $\sum a_i(m_i \otimes n_i) \in \mathbb{Q} \otimes \mathbb{Q}$, con $a_i \in \mathbb{Z},\ m_i, n_i \in \mathbb{Q}$, allora $\sum a_i(m_i \otimes n_i) = \sum a_i(m_i n_i \otimes 1) = (\sum a_i m_i n_i) \otimes 1$. Dunque tutti i tensori di $\mathbb{Q} \otimes \mathbb{Q}$ sono elementari (anzi, tutti della forma $q \otimes 1$ al variare di $q \in \mathbb{Q}$) e quindi $\tilde{f}$ è anche iniettiva. Il fatto che tutti gli elementi di $\mathbb{Q} \otimes \mathbb{Q}$ siano di quella forma rende l'isomorfismo con $\mathbb{Q}$ ancora più evidente.
- $\mathbb{Z}/(5) \otimes_{\mathbb{Z}} \mathbb{Z}/(7) \cong 0$: infatti, $5(a \otimes b) = (5a \otimes b) = 0,\ 7(a \otimes b) = a \otimes 7b = 0\ \forall a \in \mathbb{Z}/(5),\ b \in \mathbb{Z}/(7)$, quindi $a \otimes b = (5 \cdot 3 - 7 \cdot 2)(a \otimes b) = 0$. Poiché tutti i tensori elementari si annullano, il prodotto tensoriale è esso stesso nullo. Con la stessa dimostrazione otteniamo che $\mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \cong 0$ quando $\gcd(a, b) = 1$, usando l'identità di Bézout con m e n.

4.2 Estensione di scalari

Ricordiamo che, dato $f : A \longrightarrow B$ omomorfismo di anelli e M un B-modulo, possiamo dare una struttura di A-modulo a M via restrizione di scalari: $a \cdot m = f(a)m$. Abbiamo quindi un'associazione tra B-moduli e A-moduli, che trasforma anche omomorfismi di B-moduli in omomorfismi di A-moduli: dato $\varphi \in \mathrm{Hom}_B(M, N)$, notiamo che φ rispetta anche la struttura di A-modulo di M ed N: $\varphi(a \cdot m) = \varphi(f(a)m) = f(a)\varphi(m) = a \cdot \varphi(m)$. Si può dunque interpretare la restrizione di scalari come un funtore da B-moduli ad A-moduli.

B ha sia una struttura di B-modulo, sia una struttura di A-modulo, e le due strutture sono "compatibili", nel senso che l'azione di A e quella di B commutano: se $a \in A,\ b, b' \in B,\ (a \cdot b)b' = (f(a)b)b' = f(a)(bb') = a \cdot (bb')$. Si dice che B è un (A, B)-*bimodulo*. Possiamo sfruttare la doppia struttura di B per definire una sorta di "inverso" della restrizione di scalari: dato un A-modulo M, possiamo costruire un B-modulo M_B in questo modo: poniamo $M_B = M \otimes_A B,\ \cdot : B \times M_B \longrightarrow M_B,\ b \cdot (m \otimes b') = m \otimes bb'$. Questa costruzione è detta **estensione di scalari**.

Enunciamo il seguente fatto: se M è un A-modulo, P è un B-modulo ed N è un (A, B)-bimodulo, allora $(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$. La dimostrazione richiede di sviluppare la teoria delle funzioni multilineari e l'algebra multilineare. Noi lo diamo per buono, e lo usiamo per questo utile risultato:

Proposizione 4.4. Sia $(A, \mathfrak{m}, k)$ un anello locale, e siano M, N due A-moduli finitamente generati non nulli. Allora $M \otimes_A N \neq 0$.

Dimostrazione. Ricordiamo che, come conseguenza del lemma di Nakayama, abbiamo potuto definire la cardinalità di un insieme minimale di generatori per M come $\mu(M) = \dim_k(M/\mathfrak{m}M)$. Facciamo vedere che $\mu(M \otimes_A N) = \mu(M)\mu(N)$, che ovviamente dà la tesi. Per le proprietà del prodotto tensoriale abbiamo $(M \otimes_A N)/\mathfrak{m}(M \otimes_A N) \cong (M \otimes_A N) \otimes_A k \cong M \otimes_A (N \otimes_A k) \cong M \otimes_A (k \otimes_A N). \cong M \otimes_A ((k \otimes_k k) \otimes_A N)$. Osserviamo che k ha una struttura di (A, k)-bimodulo, ottenuta per restrizione di scalari tramite la proiezione da A a $k = A/\mathfrak{m}$. Usando il fatto citato sopra, si ha $M \otimes_A ((k \otimes_k k) \otimes_A N) \cong M \otimes_A (k \otimes_k (k \otimes_A N)) \cong (M \otimes_A k) \otimes_k (k \otimes_A N) \cong M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N$. Si ha quindi

$$(M \otimes_A N)/\mathfrak{m}(M \otimes_A N) \cong M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N,$$

e $\mu(M \otimes_A N) = \mu(M)\mu(N)$.

□

4.3 Moduli piatti

Sia N un A-modulo fissato. A ogni A-modulo M, possiamo associare l'A-modulo $M \otimes N$, o $N \otimes M$. Questi due moduli sono isomorfi, quindi applicare $\otimes N$ o $N \otimes$ è la stessa cosa (in teoria delle categorie si parla di "equivalenza naturale"). Vogliamo interpretare $\otimes N$ come funtore da A-moduli ad A-moduli, ma per fare ciò serve sapere come trasforma gli omomorfismi. Dati $f : M \longrightarrow N,\ g : M' \longrightarrow N'$ omomorfismi di A-moduli, definiamo $b : M \times N \longrightarrow M' \otimes N',\ b(m, n) =$

$f(m)\otimes g(n)$. b è bilineare, e induce $f\otimes g : M\otimes N \longrightarrow M'\otimes N'$, $(f\otimes g)(m\otimes n) = f(m)\otimes g(n)$. Adesso è facile associare a un omomorfismo $f : M \longrightarrow P$ un omomorfismo da $M\otimes N$ a $P\otimes N$: prendiamo $f\otimes \mathrm{id}_N$. Verifichiamo che con questa definizione $\otimes N$ è un funtore:

- $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M\otimes N}$: $\mathrm{id}_M \otimes \mathrm{id}_N(m\otimes n) = m\otimes n$, quindi è la mappa identica sui tensori elementari, e per linearità è l'identità su tutto $M\otimes N$;
- se $f\in \mathrm{Hom}(M,M')$, $f'\in \mathrm{Hom}(M',M'')$, $(f'\circ f)\otimes \mathrm{id}_N = (f'\otimes \mathrm{id}_N)\circ(f\otimes \mathrm{id}_N)$: basta osservare che in generale, se $g\in \mathrm{Hom}(N,N')$, $g'\in \mathrm{Hom}(N',N'')$, allora $((f'\circ f)\otimes(g'\circ g))(m\otimes n) = f'(f(m))\otimes g'(g(n)) = (f'\otimes g')\circ(f\otimes g)(m\otimes n)$.

Proposizione 4.5. Il funtore $\otimes N$ è esatto a destra.

Dimostrazione. Prendiamo una successione esatta $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$. Fissato un A-modulo U generico, applichiamo il funtore $\mathrm{Hom}(\bullet, U)$, che è controvariante ed esatto a sinistra, e dà la successione esatta $0 \to \mathrm{Hom}(M_2,U) \xrightarrow{g^*} \mathrm{Hom}(M,U) \xrightarrow{f^*} \mathrm{Hom}(M_1,U)$. Poniamo $U = \mathrm{Hom}(N,Q)$, con Q un A-modulo qualsiasi. Abbiamo la successione esatta

$$0 \to \mathrm{Hom}(M_2,\mathrm{Hom}(N,Q)) \to \mathrm{Hom}(M,\mathrm{Hom}(N,Q)) \to \mathrm{Hom}(M_1,\mathrm{Hom}(M,Q)).$$

Sappiamo che $\mathrm{Hom}(P,\mathrm{Hom}(N,Q)) \cong \mathrm{Bil}(P,N;Q)$ tramite $\varphi\mapsto b_\varphi$, $b_\varphi(p,n) = \varphi(p)(n)$. Inoltre, la proprietà universale di $\otimes$ dà un isomorfismo tra $\mathrm{Bil}(P,N;Q)$ e $\mathrm{Hom}(P\otimes N,Q)$, che è $f\mapsto \tilde{f}$, $\tilde{f}\circ\tau = f$. Applicando gli isomorfismi si ha $0 \to \mathrm{Hom}(M_2\otimes N,Q) \to \mathrm{Hom}(M\otimes N,Q) \to \mathrm{Hom}(M_1\otimes N,Q)$. A meno di verificare che la seconda freccia è la mappa $(g\otimes \mathrm{id}_N)^*$ e la terza freccia è $(f\otimes \mathrm{id}_N)^*$, possiamo concludere che $M_1\otimes N \xrightarrow{f\otimes \mathrm{id}_N} M\otimes N \xrightarrow{g\otimes \mathrm{id}_N} M_2\otimes N \to 0$ è esatta, che è la tesi.

□

In generale, $\otimes N$ non è esatto a sinistra: per esempio, prendendo la solita successione $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/(2) \to 0$, e tensorizzando per $\mathbb{Z}/(2)$, otteniamo $0 \to \mathbb{Z}\otimes\mathbb{Z}/(2) \xrightarrow{\times 2\otimes \mathrm{id}} \mathbb{Z}\otimes\mathbb{Z}/(2)$, e $\times 2\otimes \mathrm{id}$ non è iniettiva: infatti $(\times 2\otimes \mathrm{id})(m\otimes \overline{n}) = 2m\otimes\overline{n} = 1\otimes\overline{2mn} = 0$, ovvero $\times 2\otimes \mathrm{id}$ è la mappa nulla (e $\mathbb{Z}\otimes\mathbb{Z}/(2)$ non è 0).

Come nel caso dei moduli proiettivi, possiamo definire una classe di moduli per cui $\otimes N$ è esatto:

Definizione (Modulo piatto)**.** Un A-modulo N si dice **piatto** se il funtore $\otimes N$ è esatto.

L'esempio precedente mostra che $\mathbb{Z}/(2)$ non è uno $\mathbb{Z}$-modulo piatto.

Proposizione 4.6. Ogni modulo libero è piatto.

Dimostrazione. Iniziamo osservando che A è un A-modulo piatto: infatti, se $f : M \longrightarrow N$ è iniettiva, $f \otimes \mathrm{id}_A : M \otimes A \longrightarrow N \otimes A$ è iniettiva, in quanto, se $g : M \otimes A \longrightarrow M$, $h : N \otimes A \longrightarrow N$ sono gli isomorfismi "canonici", si verifica che $f \otimes \mathrm{id}_A = h^{-1} \circ f \circ g$. Inoltre, se M_h, N_h, P_h sono tre famiglie di moduli tali che $0 \to M_h \xrightarrow{f_h} N_h \xrightarrow{g_h} P_h \to 0$ è esatta $\forall h \in H$, possiamo definire la successione $0 \to \oplus M_h \xrightarrow{F} \oplus N_h \xrightarrow{G} \oplus P_h \to 0$, dove $F = (f_h)h \in H$, $G = (g_h)_{h \in H}$, che si verifica essere esatta (le funzioni sono applicate componente per componente, e si usa l'esattezza per ciascuna componente). Dato che il prodotto tensoriale commuta con le somme dirette, una somma diretta di moduli piatti è piatto, e si conclude osservando che ogni modulo libero è somma diretta di copie di A.

□

Proposizione 4.7. Ogni modulo proiettivo è piatto.

Dimostrazione. Se P è proiettivo, allora esiste Q tale che $P \oplus Q = F$ è libero, e quindi piatto. Consideriamo il diagramma

$$\begin{array}{ccc} M \otimes (P \oplus Q) & \xrightarrow{f \otimes (\mathrm{id}_P, \mathrm{id}_Q)} & N \otimes (P \oplus Q) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ (M \otimes P) \oplus (M \otimes Q) & \xrightarrow{(f \otimes \mathrm{id}_P, f \otimes \mathrm{id}_Q)} & (N \otimes P) \oplus (N \otimes Q) \end{array}$$

con α, β isomorfismi. Poiché $P \oplus Q$ è libero, è anche piatto, dunque la mappa orizzontale in alto è iniettiva. Segue che la mappa orizzontale in basso, $(f \otimes \mathrm{id}_P, f \otimes \mathrm{id}_Q) = \beta \circ f \otimes (\mathrm{id}_P \otimes \mathrm{id}_Q) \circ \alpha^{-1}$, è iniettiva, e quindi ciascuna componente, in particolare $f \otimes \mathrm{id}_P$, è iniettiva. Abbiamo quindi che P è piatto.

□

Vediamo un'applicazione del prodotto tensoriale a un risultato sui moduli proiettivi finitamente generati su anelli locali.

Proposizione 4.8. Sia $(A, \mathfrak{m}, k)$ un anello locale e M un A-modulo proiettivo finitamente generato. Allora M è libero.

Dimostrazione. Poiché M è un A-modulo f.g., $M/\mathfrak{m}M$ è un k-spazio vettoriale di dimensione finita; sia dunque $n = \dim_k M/\mathfrak{m}M$. Allora M ammette un sistema di generatori di cardinalità n, in quanto è finitamente generato su un anello locale (era una conseguenza del lemma di Nakayama). Possiamo dunque trovare una successione esatta

$$0 \to K \to A^n \xrightarrow{f} M \to 0,$$

con $K = \ker f$. Essendo M proiettivo, la successione spezza e $A^n \cong K \oplus M$. Tensorizzando per $k = A/\mathfrak{m}$, otteniamo $(A/\mathfrak{m})^n \cong K/\mathfrak{m}K \oplus M/\mathfrak{m}M$. Ma allora $\dim_k K/\mathfrak{m}K = \dim_k k^n - \dim_k M/\mathfrak{m}M = n - n = 0$, cioè $K/\mathfrak{m}K = 0$, ovvero $K = \mathfrak{m}K$. Inoltre K è finitamente generato, essendo un addendo diretto di A^n.

Per il lemma di Nakayama si ottiene $K = 0$, ovvero la mappa $f : A^n \longrightarrow M$ è sia iniettiva che surgettiva, ovvero M è isomorfo ad A^n, e quindi libero.

□

Concludiamo questa sezione con un esempio di un modulo piatto che non è proiettivo. $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo piatto: lo dimostreremo nel prossimo capitolo sulle localizzazioni. Però non è proiettivo, perché altrimenti sarebbe libero (gli $\mathbb{Z}$-moduli proiettivi sono liberi) e sappiamo che $\mathbb{Q}$ non è libero come $\mathbb{Z}$-modulo.

5 Localizzazione di anelli e moduli

Studiamo un nuovo modo di costruire anelli, noto come *localizzazione*, che generalizza la costruzione dei razionali a partire dagli interi. Poi con una costruzione analoga definiremo la localizzazione di un modulo, che sarà un modulo sulla localizzazione dell'anello.

5.1 Localizzazione di anelli

Definizione (Sistema moltiplicativo)**.** Sia A un anello. Un sottoinsieme $S \subseteq A$ si dice **moltiplicativamente chiuso**, o insieme/sistema moltiplicativo, se $1 \in S$ e $\forall s, t \in S \ st \in S$.

S sarà l'insieme dei possibili "denominatori" degli elementi della localizzazione, cioè elementi che saranno invertibili nel nuovo anello, dunque ha senso che sia chiuso per prodotto e contenga 1.

Successivamente definiamo la seguente relazione di equivalenza su $A \times S$: $(a, s) \sim (b, t) \iff \exists u \in S : u(at - bs) = 0$. L'insieme $(A \times S)/\sim$, munito delle operazioni $(a, s) + (b, t) = (at + bs, st)$, $(a, s) \cdot (b, t) = (ab, st)$, è un anello commutativo con identità. (Ci sarebbero diverse verifiche da fare: il fatto che $\sim$ sia una relazione di equivalenza, che le operazioni siano ben definite, e che tali operazioni soddisfino gli assiomi per un anello; tali verifiche sfruttano la moltiplicatività di S. Lo 0 di tale anello è la classe di equivalenza di $(0, 1)$, l'1 è la classe di $(1, 1)$. Per esempio, verifichiamo che la somma sia ben definita: se $(a, s) \sim (b, t)$ e $(c, v) \sim (d, w)$, allora $\exists u, z \in S : u(at - bs) = 0, \ z(cw - dv) = 0$. Dobbiamo verificare che $(a, s) + (c, v) = (av + cs, sv) \sim (bw + dt, tw) = (b, t) + (d, w)$. Poiché S è moltiplicativo, $uz \in S$; inoltre $(av + cs)(tw)(uz) = atu \cdot vwz + cwz \cdot stu = bsu \cdot vwz + dvz \cdot stu = (uz)(sv)(bw + dt)$.

Da adesso denoteremo questo anello con $S^{-1}A$, e $[(a, s)]$ con $\frac{a}{s}$. $S^{-1}A$ è detta **localizzazione** di A in S.

Iniziamo con qualche proprietà di $S^{-1}A$, per esempio, troviamo condizioni su S e A affinché $S^{-1}A = 0$. Questo accade se e solo se $\frac{0}{1} = \frac{1}{1}$, cioè se $\exists s \in S : s(0 \cdot 1 - 1 \cdot 1) = -s = 0$, ovvero se $0 \in S$. Per la moltiplicatività di S è sufficiente che $S \cap \mathcal{N}(A) \neq \emptyset$. Non è sufficiente, invece, che $S \cap \mathcal{D}(A) \neq \emptyset$.
Infatti, se $A = \mathbb{Z}/(6), \ S = \{\overline{1}, \overline{2}, \overline{4}\}$ l'insieme delle potenze di $\overline{2}$, che è moltiplicativo, allora $\overline{2} \in S \cap \mathcal{D}(A)$, ma $0 \notin S$ e quindi $S^{-1}A \neq 0$.

Un tipico esempio di insieme moltiplicativo è $S = A \setminus \mathfrak{p}$, con $\mathfrak{p} \in \operatorname{Spec} A$. Infatti, poiché $\mathfrak{p}$ è primo, $1 \notin \mathfrak{p}$, e se $a, b \notin \mathfrak{p}, \ ab \notin \mathfrak{p}$. Abbiamo già incontrato questo anello nel caso in cui $A = \mathbb{Z}, \ \mathfrak{p} = (p)$, che è $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid b \not\equiv 0 \pmod p\}$. Allora abbiamo dimostrato che era un anello locale con ideale massimale $(p)\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid a \equiv 0 \pmod p\}$. La stessa cosa vale nel caso generale: se $S = A \setminus \mathfrak{p}, \ S^{-1}A = \{\frac{a}{b} \mid b \notin \mathfrak{p}\}$. Consideriamo l'insieme $I = \mathfrak{p}S^{-1}A = \{\frac{a}{b} \in S^{-1}A \mid a \in \mathfrak{p}\}$. Questo è un ideale di $S^{-1}A$[10]: infatti $0 \in I, \ \frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \in I, \ \frac{a}{s}\frac{b}{t} = \frac{ab}{st} \in I$. Inoltre, se $\frac{a}{b} \notin I$, allora $a \notin \mathfrak{p}$, e

[10] Questa dimostrazione vale per tutti gli insiemi della forma $S^{-1}I = \{\frac{a}{b} \in S^{-1}A \mid a \in I\}$, che sono dunque ideali di A.

quindi $\frac{b}{a} \in S^{-1}A$, che è l'inverso di $\frac{a}{b}$, ovvero ogni elemento non in I è invertibile in $S^{-1}A$. Dunque $S^{-1}A$ è locale, con ideale massimale $I = \mathfrak{p}S^{-1}A$. Questo esempio motiva il nome di "localizzazione": trasforma l'ideale primo $\mathfrak{p}$ in un ideale massimale. Ma non sempre gli anelli che si ottengono in questo modo sono locali.

Un altro esempio è l'insieme $S = \mathbb{Z} \setminus \bigcup_{i=1}^{n} (p_i)$, con i p_i primi distinti. L'anello $S^{-1}\mathbb{Z}$ è $\mathbb{Z}_{(p_1,\dots,p_k)} = \{\frac{a}{b} \in \mathbb{Q} \mid b \not\equiv 0 \mod p_i \ \forall i\}$. In generale abbiamo $S = A \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i$, con $\mathfrak{p}_i$ primi. S è moltiplicativo in quanto è intersezione dei complementari dei $\mathfrak{p}_i$, e un'intersezione di sistemi moltiplicativi è un sistema moltiplicativo.

Possiamo anche considerare $S = \{a^n \mid n \in \mathbb{N}\}$, con $a \in A$ fissato. S è chiaramente moltiplicativo: poniamo $A_a = S^{-1}A$. $A_a = 0 \iff a \in \mathcal{N}(A)$; se a non è nilpotente, A_a non è banale e ha quindi un ideale massimale m. Consideriamo $\sigma : A \longrightarrow S^{-1}A,\ \alpha \mapsto \frac{\alpha}{1}$. Questo è un omomorfismo di anelli: $\frac{\alpha}{1} + \frac{\beta}{1} = \frac{\alpha+\beta}{1},\ \frac{\alpha}{1}\frac{\beta}{1} = \frac{\alpha\beta}{1}$. Allora la contrazione m^c è un ideale primo di A, e $a \notin m^c$ in quanto $\sigma(a) \in A_a^*$, e quindi non in m. Abbiamo quindi una dimostrazione alternativa del fatto che esiste un ideale primo disgiunto da un insieme moltiplicativo S (e in particolare del fatto che il nilradicale di A è l'intersezione di tutti gli ideali primi di A).

L'omomorfismo "canonico" $\sigma_S : A \longrightarrow S^{-1}A,\ a \mapsto \frac{a}{1}$ è molto utile per mettere in relazione A con la sua localizzazione. Possiamo chiederci, per esempio, se A è isomorfo a un sottoanello di $S^{-1}A$, ovvero se σ_S è iniettivo. Si ha che $a \in \ker \sigma_S \iff \frac{a}{1} = \frac{0}{1} \iff \exists s \in S : sa = 0$. Dunque σ_S è iniettivo se e solo se $\forall s \in S\ sa = 0 \implies a = 0$, ovvero S non contiene divisori di zero. Questo accade sempre se A è un dominio e $0 \notin S$ (cioè $S^{-1}A \neq 0$).

Studiamo ora gli invertibili di $S^{-1}A$. Per costruzione gli elementi di S sono invertibili in $S^{-1}A$, ovvero $\sigma_S(S) \subseteq (S^{-1}A)^*$. Non è sempre vera l'uguaglianza: per esempio, se $A = \mathbb{Z},\ S = \{6^n \mid n \in \mathbb{N}\}$, sicuramente tutte le potenze di 6 sono invertibili, ma abbiamo anche $3 \in (S^{-1}A)^*$: infatti $\frac{1}{3} = \frac{2}{6} \in S^{-1}A$, cioè 3 è invertibile, nonostante non sia un elemento di S. In generale, dato $a \in A,\ \sigma_S(a) \in (S^{-1}A)^* \iff \exists \frac{b}{s} \in S^{-1}A : \frac{a}{1}\frac{b}{s} = \frac{ab}{s} = \frac{1}{1} \iff \exists t \in S : t(ab - s) = 0 \iff a(bt) = st \in S$. La condizione generale è quindi: $\sigma_S(a) \in (S^{-1}A)^* \iff \exists x \in A : ax \in S$. Questo motiva la seguente definizione:

Definizione (Saturazione)**.** La **saturazione** di un sistema moltiplicativo S è $\overline{S} = \{\alpha \in A \mid \exists \beta \in A : \alpha\beta \in S\}$.

Notiamo che anche $\overline{S}$ è moltiplicativo: ovviamente $1 \in \overline{S}$ (anzi, $S \subseteq \overline{S}$, prendendo $\beta = 1$), e se $\alpha, \gamma \in \overline{S}$, con $\beta, \delta : \alpha\beta, \gamma\delta \in S$, poiché $\alpha\beta\gamma\delta \in S$ abbiamo $\alpha\gamma \in \overline{S}$. Per esempio, $S = A \setminus \mathfrak{p}$ ($\mathfrak{p} \in \operatorname{Spec} A$) è un insieme moltiplicativo saturato (cioè $S = \overline{S}$): infatti, se $a \in \overline{S}$ e $b \in A$ è tale che $ab \in S$, allora $a \in S$ (altrimenti $a \in \mathfrak{p} \implies ab \in \mathfrak{p}$).

Il prossimo risultato riguarda gli ideali di $S^{-1}A$, che possiamo descrivere grazie a σ_S.

Proposizione 5.1. Sia A un anello ed S un sistema moltiplicativo di A.

1. Se I è un ideale di A, $I^e = S^{-1}I = \{\frac{a}{b} \in S^{-1}A \mid a \in I\}$. Inoltre, $S^{-1}I \neq S^{-1}A \iff I \cap S = \emptyset$.

2. $I^{ec} = \bigcup_{s \in S} I : s$.

3. Se J è un ideale di $S^{-1}A$, $J^{ce} = J$. In particolare, $J = (J^c)^e = S^{-1}J^c$, quindi tutti gli ideali di $S^{-1}A$ sono l'estensione di un ideale di A.

4. La contrazione e l'estensione inducono una corrispondenza biunivoca tra ideali primi di $S^{-1}A$ e ideali primi di A che non intersecano S.

Estensione e contrazione si intendono rispetto all'omomorfismo canonico σ_S.

Dimostrazione. 1. Se $\frac{a}{s} \in S^{-1}I$, con $a \in I$, allora $\frac{a}{s} = \frac{a}{1}\frac{1}{s} \in I^e$. Ricordando che $I^e = (\sigma_S(I))$ è il più piccolo ideale contenente $\sigma_S(I)$, poiché $S^{-1}I$ è un ideale che contiene $\sigma_S(I)$ ed è contenuto in I^e, allora devono essere uguali. Per la seconda parte, se $I \cap S \neq \emptyset$, allora, preso $s \in I \cap S$, abbiamo $\frac{1}{1} = \frac{s}{s} \in S^{-1}I$. Viceversa, se $S^{-1}I = S^{-1}A$, $\frac{1}{1} = \frac{a}{s}$, $a \in I \implies \exists t \in S : t(a - s) = 0 \implies at = st$. Ma $st \in S$ e $at \in I$, quindi $st \in I \cap S$.

2. ($\subseteq$) Sia $a \in I^{ec}$; allora $\frac{a}{1} \in I^e = S^{-1}I$ (punto 1), ovvero $\frac{a}{1} = \frac{b}{s}$, $b \in I \implies \exists t \in S : t(as - b) = 0 \implies ast = bt \in I \implies a \in I : st \subseteq \bigcup_{s \in S} I : s$.

   ($\supseteq$) Sia $a \in I : s$ per qualche $s \in S$. Allora $as \in I \implies \frac{as}{1} \in I^e$ e quindi $\frac{a}{1} \in I^e$, cioè $a \in I^{ec}$.

3. Sappiamo già che $J \supseteq J^{ce}$. Per l'inclusione opposta, sia $\frac{a}{s} \in J$. Allora $\frac{a}{1} \in J$ e $a \in J^c$, dunque $\frac{a}{s} \in S^{-1}J^c = J^{ce}$.

4. È già noto che la contrazione di un ideale primo è un ideale primo; in più, se Q è un primo di $S^{-1}A$, Q^c non può intersecare S: se $s \in Q^c \cap S$, $\frac{s}{1} \in Q \cap (S^{-1}A)^*$, assurdo. Dobbiamo quindi dimostrare che, se P è un primo di A con $P \cap S = \emptyset$, allora $P^e = S^{-1}P$ è un primo di $S^{-1}A$. Siano $\frac{a}{s}$, $\frac{b}{t} : \frac{ab}{st} \in S^{-1}P$. Quindi $\frac{ab}{st} = \frac{p}{u}$, $p \in P$, $u \in S$, ed esiste $v \in S : abuv = pstv$. Poiché $p \in P$, $pstv = abuv \in P$, e per la primalità di P uno tra a, b, u, v appartiene a P. Siccome $P \cap S = \emptyset$ e $u, v \in S$, deve essere $a \in P$ o $b \in P$, che implica $\frac{a}{s} \in S^{-1}P$ o $\frac{b}{t} \in S^{-1}P$, come voluto.

□

Esempio. *Sia $A = \mathbb{Z}$, $S = A \setminus (p)$, cioè $S^{-1}A = \mathbb{Z}_{(p)}$. Descriviamo i suoi ideali: sappiamo che gli ideali propri di $\mathbb{Z}_{(p)}$ corrispondono agli ideali di $\mathbb{Z}$ disgiunti da S, cioè contenuti in p. Se $(n) \subseteq (p)$, allora $p|n$, e possiamo scrivere $n = \alpha p^t$, $t > 0$, $\gcd(\alpha, p) = 1$. (Ovviamente, se $n = 0$, $(n)^e = (0)$). Allora α è invertibile in $\mathbb{Z}_{(p)}$, ovvero $(n)^e = (p^t)^e = (p^e)^t$ (estensione e prodotto commutano).*

Esempio. *Sia $A = \mathbb{Z}/(12)$, e sia S l'insieme delle potenze di $\overline{2}$: $S = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$. Vogliamo calcolare $S^{-1}A$. Per prima cosa, elenchiamo gli ideali di $S^{-1}A$: i suoi ideali propri corrispondono agli ideali di A che non intersecano S. Gli ideali di A sono $(\overline{0}), (\overline{1}), (\overline{2}), (\overline{3}), (\overline{4}), (\overline{6})$. Abbiamo subito che $(\overline{2})$ e $(\overline{4})$ esplodono nella localizzazione, in quanto intersecano S; inoltre $\overline{3}, \overline{6}, \overline{0}$ sono associati in $S^{-1}A$: $\overline{6} = \overline{3} \cdot \overline{2},\ \overline{0} = \overline{3} \cdot \overline{4}$. Dunque $S^{-1}A$ possiede solo gli ideali $(\overline{0})^e$ e $(\overline{1})^e$, ovvero è un campo. Quindi per identificarlo ci basta sapere quanti elementi ha. Osserviamo che $\frac{1}{1} \neq \frac{1}{2}$ (1 non è annullato da alcun elemento di S), ma $\frac{1}{1} = \frac{1}{4}$, dato che $\overline{3} \cdot \overline{4} = \overline{0}$. Si verifica che, a meno di equivalenza, gli unici elementi di $S^{-1}A$ sono $0, 1, \frac{1}{2}$, ovvero $S^{-1}A$ è il campo con 3 elementi.*

C'è un modo più semplice per calcolare $S^{-1}A$ nel caso in cui A è finito, che sfrutta il seguente fatto: se A è finito, $\sigma_S : A \longrightarrow S^{-1}A$ è surgettivo. Infatti, essendo A finito, anche S e $A \times S$ sono insiemi finiti, ed essendo $S^{-1}A$ un quoziente (insiemistico) di $A \times S$, è anch'esso un anello finito, e dunque il suo gruppo delle unità è finito. Allora tutti gli invertibili di $S^{-1}A$ hanno ordine finito (teorema di Lagrange). Se ora prendiamo $\frac{a}{s} \in S^{-1}A$, ed $n \in \mathbb{N} : (\frac{1}{s})^n = \frac{1}{1}$, abbiamo $\frac{a}{s} = \frac{as^{n-1}}{s^n} = \frac{as^{n-1}}{1} = \sigma_S(as^{n-1})$, dunque σ_S è surgettivo. In questo caso $S^{-1}A \cong A/\ker\sigma_S$. Applicando questo fatto all'esempio precedente, $\overline{a} \in \ker\sigma_S \iff \exists \overline{s} \in S : \overline{as} = \overline{0}$, cioè $12|a \cdot 2^n$ per qualche n e quindi $3|a$. Abbiamo dunque che $\ker\sigma_S = (\overline{3})$, e $S^{-1}A \cong (\mathbb{Z}/(12))/(\overline{3}) \cong \mathbb{Z}/(3)$.

L'estensione di ideali tramite σ_S gode di altre proprietà:

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. È una proprietà generale dell'estensione di ideali.
2. Come 1.
3. Dal caso generale dell'estensione di ideali si deduce l'inclusione $\subseteq$. Per l'inclusione opposta, un elemento x di $S^{-1}I \cap S^{-1}J$ si può scrivere come $x = \frac{i}{s} = \frac{j}{t}$, con $i \in I,\ j \in J$. Quindi $\exists u \in S : itu = jsu$. Chiaramente $itu = jsu \in I \cap J$, dunque $x = \frac{i}{s} = \frac{itu}{stu} \in S^{-1}(I \cap J)$.
4. ($\subseteq$) Sia $\frac{a}{s} \in S^{-1}\sqrt{I}$, con $a \in \sqrt{I}$. Allora $a^n \in I$ per qualche n, e $(\frac{a}{s})^n = \frac{a^n}{s^n} \in S^{-1}I$, dunque $\frac{a}{s} \in \sqrt{S^{-1}I}$.

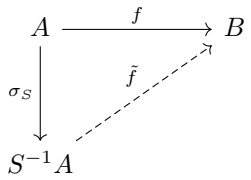
   ($\supseteq$) Se $\frac{a}{s} \in \sqrt{S^{-1}I}$, $\exists n \in \mathbb{N} : \frac{a^n}{s^n} \in S^{-1}I$. Allora $\frac{a^n}{s^n} = \frac{i}{t}$ per qualche $i \in I,\ t \in S$, quindi $\exists u \in S : a^n tu = s^n iu$. Poiché $i \in I$, anche $a^n tu \in I$, e $a^n t^n u^n = (atu)^n \in I$. Abbiamo allora che $atu \in \sqrt{I}$, che implica $\frac{a}{s} = \frac{atu}{stu} \in S^{-1}\sqrt{I}$.

□

Come il prodotto tensoriale, anche la localizzazione di un anello è caratterizzata da una proprietà universale.

Teorema 5.2 (Proprietà universale della localizzazione)**.** Sia A un anello ed S un sistema moltiplicativo di A.

1. Fissiamo $f : A \longrightarrow B$ omomorfismo di anelli tale che $f(S) \subseteq B^*$. Allora $\exists! \tilde{f} : S^{-1}A \longrightarrow B$ che fa commutare il diagramma



2. Se $f : A \longrightarrow B$ è un omomorfismo di anelli tale che:

   - $f(S) \subseteq B^*$;
   - $\forall b \in B \ \exists a \in A,\ s \in S : b = f(a)f(s)^{-1}$;
   - $a \in \ker f \iff \exists s \in S : as = 0$;

   allora B ed $S^{-1}A$ sono isomorfi tramite $\tilde{f}$.

Dimostrazione. 1. Una $\tilde{f}$ come nella tesi deve essere tale che

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

quindi, se esiste, è unica. Se definiamo $\tilde{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$, per costruzione fa commutare il diagramma. Inoltre l'elemento $f(s)^{-1}$ è in B in quanto $f(S) \subseteq B^*$. Verifichiamo che è ben definita: se $\frac{a}{s} = \frac{b}{t}$, e $u \in S$ è tale che $u(at - bs) = 0$, allora $0 = f(u)[f(a)f(t) - f(b)f(s)]$. Per l'invertibilità di $f(u)$, l'espressione tra parentesi quadre è 0; riarrangiando e moltiplicando ambo i membri per $f(s)^{-1}f(t)^{-1}$ si ottiene $\tilde{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1} = f(b)f(t)^{-1} = \tilde{f}\left(\frac{b}{t}\right)$. Il fatto che $\tilde{f}$ sia un omomorfismo segue dalla sua definizione e dal fatto che f è un omomorfismo.

2. Poiché $f(S) \subseteq B^*$, per il punto 1 esiste $\tilde{f} : S^{-1}A \longrightarrow B$ con $f = \tilde{f} \circ \sigma_S$. $\tilde{f}$ è surgettiva in quanto, preso $b \in B$, per la seconda ipotesi esistono $a \in A,\ s \in S$ tali che $b = f(a)f(s)^{-1} = \tilde{f}(\frac{a}{1})\tilde{f}(\frac{1}{s}) = \tilde{f}(\frac{a}{s})$. Infine $\tilde{f}$ è iniettiva, dato che, se $\frac{a}{s} \in \ker \tilde{f},\ \tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1} = 0$ e quindi $f(a) = 0$, cioè $a \in \ker f$. Per la terza ipotesi esiste $s' \in S : as' = 0$, e si ha $\frac{a}{s} = \frac{as'}{ss'} = 0$.

□

Sia A un anello e $\mathfrak{p} \in \operatorname{Spec} A$. Abbiamo due modi di ottenere un campo da A e $\mathfrak{p}$: quozientare per $\mathfrak{p}$, ottenendo il dominio d'integrità $A/\mathfrak{p}$, e poi prendere il campo dei quozienti $Q(A/\mathfrak{p})$ (cioè localizzare nel primo di $A/\mathfrak{p}$ $(\overline{0})$), oppure

localizzare in $\mathfrak{p}$, ottenendo l'anello locale $A_\mathfrak{p}$, e poi quozientare per il suo ideale massimale $\mathfrak{p}A_\mathfrak{p}$. Vogliamo mostrare che "localizzare e quozientare commutano", cioè che questi due modi restituiscono campi isomorfi.

Sia $f = \pi \circ \sigma_S,\ f : A \xrightarrow{\sigma_S} A_\mathfrak{p} \xrightarrow{\pi} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, con $S = A \setminus \mathfrak{p}$. Il nucleo di f è la contrazione di $\mathfrak{p}A_\mathfrak{p} = \mathfrak{p}^e$ tramite σ_S, cioè $\ker f = \mathfrak{p}^{ec} = \bigcup_{s\in S} \mathfrak{p} : s$. Osserviamo che $\mathfrak{p}^{ec} = \bigcup_{s\in S} \mathfrak{p} : s = \mathfrak{p}$: infatti, $\mathfrak{p} = \mathfrak{p} : 1 \subseteq \bigcup_{s\in S} \mathfrak{p} : s$, e se $x \in \mathfrak{p} : s$ per qualche $s \in S$, allora $xs \in \mathfrak{p}$, quindi $x \in \mathfrak{p}$ poiché $\mathfrak{p}$ è primo e $s \notin \mathfrak{p}$. Si ha dunque $\ker f = \mathfrak{p}$, e per il primo teorema di isomorfismo esiste un'unica $\varphi : A/\mathfrak{p} \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ iniettiva con $\varphi \circ \pi_\mathfrak{p} = f$, con $\pi_\mathfrak{p}$ la proiezione di A modulo $\mathfrak{p}$. Ora, sia $T = A/\mathfrak{p} \setminus (\overline{0})$, in modo che $T^{-1}A/\mathfrak{p} = Q(A/\mathfrak{p})$. Se $\overline{a} \in T$, allora $a \notin \mathfrak{p}$, e $\varphi(\overline{a}) = f(a) \neq 0$, dato che $\ker f = \mathfrak{p}$. Siccome $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ è un campo, $f(a)$ è invertibile, dunque $\varphi(T) \subseteq (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})^*$. Per la proprietà universale $\exists\tilde{\varphi} : T^{-1}A/\mathfrak{p} \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ tale che $\tilde{\varphi} \circ \sigma_T = \varphi$. Mostriamo ora che $\tilde{\varphi}$ è un isomorfismo. L'iniettività di $\tilde{\varphi}$ segue da quella di φ: il criterio è $a \in \ker\varphi \iff \exists s \in S : as = 0$, e se φ è iniettiva $a = 0$, e basta scegliere $s = 1$. Per la surgettività, sia $\overline{a/s} \in A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, con $a \in A$ ed $s \in S$, e notiamo che $\varphi(\overline{a})\varphi(\overline{s})^{-1} = f(a)f(s)^{-1} = \overline{a/1} \cdot \overline{1/s} = \overline{a/s}$, come voluto. (Qui $\overline{a/s}$ è una classe di resto modulo $\mathfrak{p}A_\mathfrak{p}$, mentre $\overline{a}, \overline{s}$ sono classi di resto modulo $\mathfrak{p}$).

5.2 Localizzazione di moduli

Siano M un A-modulo ed S un sistema moltiplicativo di A. Possiamo ripetere la costruzione per ottenere la localizzazione di M in S: definiamo $S^{-1}M = (M \times S)/\sim$, dove $(m, s) \sim (n, t) \iff \exists u \in S : u(tm - sn) = 0$. Anche qui si usa la notazione $\frac{m}{s}$. Possiamo definire una struttura di $S^{-1}A$-modulo su $S^{-1}M$, tramite l'azione $\cdot : S^{-1}A \times S^{-1}M \longrightarrow S^{-1}M,\ (\frac{a}{s}, \frac{m}{t}) \mapsto \frac{am}{st}$.

Anche la localizzazione di moduli ha una proprietà universale, ma bisogna fare qualche modifica rispetto al caso degli anelli. Sia $f : M \longrightarrow N$ un omomorfismo di A-moduli. Possiamo ancora definire l'omomorfismo canonico $\sigma_S : M \longrightarrow S^{-1}M,\ m \mapsto \frac{m}{1}$, e vorremmo trovare $\tilde{f} : S^{-1}M \longrightarrow N$ omomorfismo di $S^{-1}A$-moduli tale che $\tilde{f} \circ \sigma_S = f$. Il problema è definire una struttura di $S^{-1}A$-modulo su N. L'analogo della condizione $f(S) \subseteq B^*$ è che, per ogni $s \in S$, la moltiplicazione per $s,\ \times s : N \longrightarrow N,\ n \mapsto sn$, è invertibile. Sotto questa ipotesi possiamo definire $\cdot : S^{-1}A \times N \longrightarrow N,\ \frac{a}{s} \cdot n = as^{-1}(n)$, dove s^{-1} è l'inverso della moltiplicazione per s. Verifichiamo che l'azione è ben definita: se $\frac{a}{s} = \frac{b}{t}$ e $u \in S$ è tale che $u(ta - sb) = 0,\ u(ta - sb)n = 0\ \forall n \in N$. La moltiplicazione per u è invertibile, quindi deve essere $(ta - sb)n = 0$. Applicando s^{-1} e t^{-1} e usando il fatto che commutano (la composizione in entrambi i sensi è $(st)^{-1}$), otteniamo $s^{-1}(an) - t^{-1}(bn) = as^{-1}(n) - bt^{-1}(n) = 0$, cioè $as^{-1}n = bt^{-1}(n)$. Infine, si verifica che $\tilde{f} : S^{-1}M \longrightarrow N,\ \tilde{f}(\frac{m}{s}) = \frac{f(m)}{s}$, è ben definita e soddisfa la proprietà richiesta.

Possiamo dare una condizione sufficiente affinché $S^{-1}M = 0$: basta che $S \cap \mathrm{Ann}(M) \neq \emptyset$. Infatti, se $s \in S \cap \mathrm{Ann}(M),\ \forall \frac{m}{t} \in S^{-1}M\ \frac{m}{t} = \frac{sm}{st} = 0$. Tale condizione è anche necessaria se assumiamo che M sia *finitamente generato*. Se

$M = \langle m_1, ..., m_r \rangle_A$, allora $S^{-1}M = \langle \frac{m_1}{1}, ..., \frac{m_r}{1} \rangle_{S^{-1}A}$. Supponendo che $S^{-1}M = 0$, $\forall 1 \leq i \leq r$ $\frac{m_i}{1} = 0$, ed esiste $s_i \in S$ tale che $s_i m_i = 0$. Posto $s = s_1 s_2 \cdots s_r \in S$, $t_i = \frac{s}{s_i}$, per ogni i abbiamo $sm_i = t_i s_i m_i = 0$, quindi s annulla un insieme di generatori di M e $s \in \mathrm{Ann}(M)$.

Questo non è vero se M non è finitamente generato. Per esempio, sia M lo $\mathbb{Z}$-modulo $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}/(2^i)$. L'elemento $e_i \in M$ con zeri ovunque tranne che alla coordinata i è annullato dai multipli di 2^i, quindi $\mathrm{Ann}(e_i) = (2^i)$ e $\mathrm{Ann}(M) \subseteq \bigcap_i \mathrm{Ann}(e_i) = \bigcap_i (2^i) = 0$. Sia ora $S = \{2^i \mid i \in \mathbb{N}\}$. $0 \notin S$, dunque $S \cap \mathrm{Ann}(M) = 0$, ma, se $\alpha \in S^{-1}M$, è della forma $\frac{1}{2^r}(\overline{a_1}, ..., \overline{a_k}, 0, 0, ...)$, e α è annullato da $2^{r+k} \in S$, che rende il modulo $S^{-1}M$ nullo.

Dato un A-modulo M, la localizzazione $S^{-1}M$ permette di estendere l'anello degli scalari da A a $S^{-1}A$. Un altro modo naturale per fare ciò è l'estensione di scalari data dal prodotto tensoriale $M \otimes_A S^{-1}A$. Mostriamo che localizzazione e prodotto tensoriale danno lo stesso risultato:

Proposizione 5.3. Sia A un anello, S un sistema moltiplicativo di A e M un A-modulo. Allora $M \otimes_A S^{-1}A \cong S^{-1}M$.

Dimostrazione. Definiamo $f : M \times S^{-1}A \longrightarrow S^{-1}M$, $f(m, \frac{a}{s}) = \frac{am}{s}$. Si verifica che la mappa è ben definita, bilineare e surgettiva, e induce $\tilde{f} : M \otimes_A S^{-1}A \longrightarrow S^{-1}M$, $m \otimes \frac{a}{s} = \frac{am}{s}$. Mostriamo ora che tutti i tensori di $M \otimes_A S^{-1}A$ sono elementari. Se $\sum m_i \otimes \frac{a_i}{s_i} \in M \otimes_A S^{-1}A$, posto $s = s_1 s_2 \cdots s_r$, $t_i = \frac{s}{s_i}$, si ha $\sum m_i \otimes \frac{a_i}{s_i} = \sum m_i \otimes \frac{t_i m_i}{s} = (\sum t_i a_i m_i) \otimes \frac{1}{s} = m \otimes \frac{1}{s}$. Adesso è facile verificare l'iniettività: $\tilde{f}(m \otimes \frac{1}{s}) = 0 \iff \frac{m}{s} = 0 \iff \exists t \in S : tm = 0$, e allora $m \otimes \frac{1}{s} = m \otimes \frac{t}{ts} = tm \otimes \frac{1}{ts} = 0$.

□

5.3 Il funtore S^{-1}

In virtù del risultato appena dimostrato, e sfruttando la funtorialità del prodotto tensoriale, possiamo interpretare S^{-1} come un funtore da A-moduli a $S^{-1}A$-moduli: a un omomorfismo $f : M \longrightarrow N$ associamo

$$f \otimes \mathrm{id}_{S^{-1}A} : M \otimes S^{-1}A \longrightarrow N \otimes S^{-1}A, \ (m, \frac{a}{s}) \mapsto (f(m), \frac{a}{s}),$$

e via l'isomorfismo tra $M \otimes S^{-1}A$ e $S^{-1}M$, definiamo

$$S^{-1}f : S^{-1}M \longrightarrow S^{-1}N, \ \frac{am}{s} \mapsto \frac{af(m)}{s} = \frac{f(am)}{s}.$$

Quindi $S^{-1}f$ applica f al numeratore e lascia invariato il denominatore.

Le proprietà del prodotto tensoriale garantiscono che il funtore S^{-1} è esatto a destra (anche se non è complicato dimostarlo per via diretta). In realtà vale la seguente:

Proposizione 5.4. Il funtore S^{-1} è esatto.

Dimostrazione. Basta mostrare l'esattezza a sinistra. Sia dunque $f : M \longrightarrow N$ iniettiva: vogliamo mostrare che $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ è anch'essa iniettiva. Sia $\frac{m}{s} \in \ker S^{-1}f$. Allora $S^{-1}f(\frac{m}{s}) = \frac{f(m)}{s} = 0$, quindi $\exists t \in S : tf(m) = f(tm) = 0$, ovvero $tm \in \ker f$. Per l'iniettività di f $tm = 0$, dunque $\frac{m}{s} = \frac{tm}{ts} = 0$. □

Un'immediata conseguenza delle due proposizioni precedenti è che, se A è un anello e S un sistema moltiplicativo di A, allora $S^{-1}A$ è un A-modulo piatto. (Per esempio, $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo piatto).

Osservazione. Un'altra proprietà che tornerà utile è questa: se M, N sono due A-moduli, $S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N$. Infatti, usando la struttura di $(A, S^{-1}A)$-bimodulo di $S^{-1}A$, si ottiene

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

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

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

Dimostriamo altre utili proprietà della localizzazione:

1. se $M, N \subseteq P$, $S^{-1}(M + N) = S^{-1}M + S^{-1}N$;
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$;
3. se $N \subseteq M$, $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$;
4. se M è finitamente generato, $\mathrm{Ann}_{S^{-1}A}(S^{-1}M) = S^{-1}\,\mathrm{Ann}_A(M)$;
5. se N è finitamente generato, $S^{-1}(M : N) = S^{-1}M : S^{-1}N$.

Le prime due affermazioni implicano immediatamente che la localizzazione commuta con le somme dirette.

Dimostriamo 3, 4, 5.

3. Consideriamo la successione esatta $0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0$. Poiché la localizzazione preserva l'esattezza, anche la successione $0 \to S^{-1}N \xrightarrow{S^{-1}i} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/N) \to 0$ è esatta. Abbiamo anche la successione esatta $0 \to S^{-1}N \xrightarrow{j} S^{-1}M \xrightarrow{\pi'} S^{-1}M/S^{-1}N \to 0$. Fondiamo le due successioni nel diagramma commutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S^{-1}N & \longrightarrow & S^{-1}M & \longrightarrow & S^{-1}(M/N) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{S^{-1}N}} & & \downarrow{\scriptstyle \mathrm{id}_{S^{-1}M}} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & S^{-1}N & \longrightarrow & S^{-1}M & \longrightarrow & S^{-1}M/S^{-1}N & \longrightarrow & 0
\end{array}$$

dove $f : S^{-1}(M/N) \longrightarrow S^{-1}M/S^{-1}N$ è definita come $f(\frac{m+N}{s}) = \frac{m}{s} + S^{-1}N$. (Con $m + N$ si intende la classe di m modulo N). Si verifica che f è un

omomorfismo ben definito che fa commutare il diagramma. Per il lemma del serpente f è un isomorfismo.

4. Procediamo per induzione sul numero minimo n di generatori di M.

Passo base, $n = 1$: $M = \langle m \rangle_A$, e $\operatorname{Ann}_A(M) = \operatorname{Ann}_A(m)$. Se $a \in \operatorname{Ann}_A(M)$ e $s \in S$, $\frac{a}{s}\frac{m}{1} = \frac{am}{s} = 0$, e $\frac{m}{1}$ genera $S^{-1}M$. Quindi si ha che $S^{-1}\operatorname{Ann}_A(M) \subseteq \operatorname{Ann}_{S^{-1}A}(S^{-1}M)$. Viceversa, se $\frac{a}{s} \in \operatorname{Ann}_{S^{-1}A}(S^{-1}M)$, $\frac{a}{s}\frac{m}{1} = \frac{am}{s} = 0$, dunque $\exists t \in S : atm = 0$, e $at \in \operatorname{Ann}_A(M)$. Ma allora $\frac{a}{s} = \frac{at}{st} \in S^{-1}\operatorname{Ann}(M)$.

Passo induttivo, $n - 1 \implies n$: sia $M = \langle m_1, ..., m_n \rangle$, e poniamo $N_1 = \langle m_1, ..., m_{n-1} \rangle$, $N_2 = \langle m_n \rangle$. Allora $M = N_1 + N_2$, e per ipotesi induttiva e passo base la tesi è vera per N_1 ed N_2 rispettivamente. Notiamo inoltre che, se $N, P \subseteq M$, $\operatorname{Ann}(N + P) = \operatorname{Ann}(N) \cap \operatorname{Ann}(P)$: infatti a annulla tutti gli elementi di $N + P$ se e solo se annulla gli elementi di N e di P. Quindi abbiamo

$$S^{-1}\operatorname{Ann}_A(M) = S^{-1}\operatorname{Ann}_A(N_1 + N_2) = S^{-1}(\operatorname{Ann}_A(N_1) \cap \operatorname{Ann}_A(N_2)) =$$

$$S^{-1}\operatorname{Ann}_A(N_1) \cap S^{-1}\operatorname{Ann}_A(N_2) = \operatorname{Ann}_{S^{-1}A}(S^{-1}N_1) \cap \operatorname{Ann}_{S^{-1}A}(S^{-1}N_2) =$$

$$\operatorname{Ann}_{S^{-1}A}(S^{-1}N_1 + S^{-1}N_2) = \operatorname{Ann}_{S^{-1}A}(S^{-1}(N_1 + N_2)) = \operatorname{Ann}_{S^{-1}A}(S^{-1}M).$$

5. L'osservazione chiave è che $M : N = \operatorname{Ann}_A((M + N)/M)$. Infatti, $a \in M : N \iff aN \subseteq M \iff a(M + N) \subseteq M \iff a(M + N)/M = 0$. Inoltre N è f.g., e considerando la mappa $N \hookrightarrow M + N \to (M + N)/M$, le immagini dei generatori di N generano $(M + N)/M$. Dunque anche $(M + N)/M$ è f.g. Usando tale osservazione e il punto 4 si ottiene

$$S^{-1}(M : N) = S^{-1}\operatorname{Ann}_A((M + N)/M) = \operatorname{Ann}_{S^{-1}A}(S^{-1}((M + N)/M)) =$$

$$\operatorname{Ann}_{S^{-1}A}((S^{-1}M + S^{-1}N)/S^{-1}M) = S^{-1}M : S^{-1}N.$$

La 5. è falsa se N non è finitamente generato. Sia $A = K[t, \frac{x}{t^n} \mid n \in \mathbb{N}]$, con K un campo. Siano inoltre $M = \langle x \rangle_A$, $N = \langle \frac{x}{t^n} \mid n \in \mathbb{N} \rangle_A$, $S = \{t^n \mid n \in \mathbb{N}\}$. Osserviamo che $\frac{1}{t^n} \notin A$. Si ha che

$$M : N = \{a \in A \mid a\frac{x}{t^n} \in M \ \forall n \in \mathbb{N}\} = \{a \in A \mid \frac{a}{t^n} \in A \ \forall n \in \mathbb{N}\} = N,$$

poiché t non è invertibile in A. Quindi $S^{-1}(M : N) = S^{-1}N$. Però $S^{-1}M = S^{-1}N$, in quanto $\frac{x}{t^n} = \frac{1}{t^n}x \in S^{-1}M$, e allora abbiamo $S^{-1}M : S^{-1}N = S^{-1}N : S^{-1}N = S^{-1}A \neq S^{-1}N = S^{-1}(M : N)$, dato che $1 \notin S^{-1}N$.

Vediamo qualche applicazione dell'esempio più importante di localizzazione, quella negli ideali primi di A.

Definizione (Supporto)**.** Sia M un A-modulo. Il **supporto** di M è l'insieme

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \mid M_\mathfrak{p} \neq 0\}.$$

Se M è finitamente generato, $M_\mathfrak{p} \neq 0 \iff \operatorname{Ann}(M) \cap A \setminus \mathfrak{p} = \emptyset \iff \operatorname{Ann}(M) \subseteq \mathfrak{p}$. In tal caso $\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \mid \operatorname{Ann}(M) \subseteq \mathfrak{p}\}$.

Esempio. *Sia M lo $\mathbb{Z}$-modulo $\mathbb{Z}/(18) \oplus \mathbb{Z}/(12)$. L'annullatore di M è generato dal minimo comune multiplo di 18 e 12, 36. Quindi i primi che lo contengono, e che costituiscono il supporto di M, sono $(2), (3)$. Per le proprietà della localizzazione abbiamo $M_{(2)} \cong \mathbb{Z}_{(2)}/(18)_{(2)} \oplus \mathbb{Z}_{(2)}/(12)_{(2)} = \mathbb{Z}_{(2)}/(2)_{(2)} \oplus \mathbb{Z}_{(2)}/(4)_{(2)} \cong (\mathbb{Z}/(2))_{(2)} \oplus (\mathbb{Z}/(4))_{(2)} = \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$. Similmente, si trova che $M_{(3)} \cong \mathbb{Z}/(9) \oplus \mathbb{Z}/(3)$. Notiamo che se M è un gruppo abeliano finitamente generato, trattandolo come uno $\mathbb{Z}$-modulo e localizzando in ciascun primo non nullo del supporto, otteniamo che $M_{(p)}$ è il p-Sylow di M.*

Proposizione 5.5. Siano M, N, P tre A-moduli.

1. Se $0 \to M \to N \to P \to 0$ è una successione esatta, $\operatorname{Supp} N = \operatorname{Supp} M \cup \operatorname{Supp} P$.
2. Se M, N sono finitamente generati, $\operatorname{Supp}(M \otimes N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

Dimostrazione.
1. La localizzazione preserva l'esattezza, quindi la successione $0 \to M_\mathfrak{p} \to N_\mathfrak{p} \to P_\mathfrak{p} \to 0$ è esatta. Dunque $N_\mathfrak{p} \neq 0 \iff M_\mathfrak{p} \neq 0 \vee P_\mathfrak{p} \neq 0$, da cui la tesi.
2. Sappiamo che localizzazione e prodotto tensoriale "commutano", quindi $(M \otimes_A N)_\mathfrak{p} \cong M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}$, che è un prodotto tensoriale di moduli f.g. su un anello locale. Ma abbiamo dimostrato che sotto tali ipotesi $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \neq 0 \iff M_\mathfrak{p} \neq 0 \wedge N_\mathfrak{p} \neq 0$, perciò $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

□

5.4 Proprietà locali

La localizzazione nei primi di A è così importante perché permette di dimostrare alcune proprietà di moduli su anelli qualsiasi (dette *proprietà locali*) dimostrandole solo sulle sue localizzazioni. Questo può facilitare molto tali dimostrazioni, in quanto abbiamo strumenti molto potenti che funzionano bene per moduli su anelli locali (*in primis* il lemma di Nakayama).

Definizione (Proprietà locale)**.** Una proprietà P di un A-modulo si dice **locale** se è vero questo: P è vera per l'A-modulo M se e solo se P è vera per l'$A_\mathfrak{p}$-modulo $M_\mathfrak{p}$.

Vediamo un esempio di proprietà locale tanto semplice quanto fondamentale: essere nullo.

Proposizione 5.6. Essere l'A-modulo nullo è una proprietà locale.

Dimostrazione. Ovviamente tutte le localizzazioni di 0 sono nulle, vediamo il viceversa. Sia $m \in M$. Poiché $M_\mathfrak{p} = 0 \ \forall \mathfrak{p} \in \operatorname{Spec} A$, $\frac{m}{1} = 0$, ed esiste $t_\mathfrak{p} \in A \setminus \mathfrak{p}$ tale che $t_\mathfrak{p} m = 0$. Abbiamo allora che $\operatorname{Ann}(m)$ non è contenuto in nessun primo di A, e in particolare in nessun ideale *massimale* di A, quindi $\operatorname{Ann}(m) = A$, cioè $m = 0$.

□

In questo caso è sufficiente controllare che $M_{\mathfrak{m}} = 0$ per ogni $\mathfrak{m}$ massimale, invece che su tutti i primi.

Come conseguenza, abbiamo che una proprietà è locale se è "determinata dall'annullarsi di qualcosa". Per esempio, essere un anello ridotto è una proprietà locale: infatti, A è ridotto $\iff \mathcal{N}(A) = (0) \iff (\mathcal{N}(A))_{\mathfrak{p}} = \mathcal{N}(A_{\mathfrak{p}}) = (0) \iff A_{\mathfrak{p}}$ è ridotto. (Abbiamo usato il fatto che localizzazione e (nil)radicale commutano).

Proposizione 5.7. L'esattezza è una proprietà locale.

Dimostrazione. Sappiamo già che localizzare preserva l'esattezza. Prendiamo una successione $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$, e supponiamo che $\forall \mathfrak{p} \in \operatorname{Spec} A$ $0 \to M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} P_{\mathfrak{p}} \to 0$ è esatta. Questo equivale alle tre condizioni $\ker f_{\mathfrak{p}} = 0$, $\ker g_{\mathfrak{p}} / \operatorname{Im} f_{\mathfrak{p}} = 0$, $P_{\mathfrak{p}} / \operatorname{Im} g_{\mathfrak{p}} = 0$. Per concludere basta dimostrare che, se $f : M \longrightarrow N$ è un omomorfismo di A-moduli, e $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ è l'omomorfismo indotto sulle localizzazioni, allora $\ker S^{-1}f = S^{-1} \ker f$, $\operatorname{Im} S^{-1}f = S^{-1} \operatorname{Im} f$. Infatti, se vale questo abbiamo $(\ker f)_{\mathfrak{p}} = \ker f_{\mathfrak{p}} = 0$, $(\ker g / \operatorname{Im} f)_{\mathfrak{p}} \cong \ker g_{\mathfrak{p}} / \operatorname{Im} f_{\mathfrak{p}} = 0$, $(P / \operatorname{Im} g)_{\mathfrak{p}} \cong P_{\mathfrak{p}} / \operatorname{Im} g_{\mathfrak{p}} = 0$ e, poiché annullarsi è una proprietà locale, $\ker f = 0$, $\ker g / \operatorname{Im} f = 0$, $P / \operatorname{Im} g = 0$, che corrisponde all'esattezza della successione di partenza.

$S^{-1} \ker f = \ker S^{-1} f$: si ha che

$$\frac{m}{s} \in \ker S^{-1}f \iff S^{-1}f(\frac{m}{s}) = \frac{f(m)}{s} = 0 \iff \exists t \in S : tf(m) = f(tm) = 0$$

$$\iff tm \in \ker f \iff \frac{tm}{ts} = \frac{m}{s} \in S^{-1} \ker f.$$

$S^{-1} \operatorname{Im} f = \operatorname{Im} S^{-1} f$: abbiamo che

$$\frac{n}{s} \in \operatorname{Im} S^{-1}f \iff \exists m \in M,\ t \in S : \frac{n}{s} = S^{-1}f(\frac{m}{t}) = \frac{f(m)}{t} = \iff \exists u \in S :$$

$$usf(m) = utn = f(usm) \iff \frac{f(usm)}{uts} = \frac{utn}{uts} = \frac{n}{s} \in S^{-1} \operatorname{Im} f.$$

□

Esistono anche proprietà non locali: diamo due esempi.

- Essere un dominio non è una proprietà locale. Infatti, $A = \mathbb{Z}/(10)$ non è un dominio, e ha solo due ideali primi: $(\overline{2})$ e $(\overline{5})$. Ma $(\mathbb{Z}/(10))_{(\overline{2})} \cong \mathbb{Z}/(5)$, e $(\mathbb{Z}/(10))_{(\overline{5})} \cong \mathbb{Z}/(2)$, che sono dei domini.

- Essere un anello noetheriano non è una proprietà locale. Sia A l'anello $\mathbb{Z}/(2)[x_i \mid i \in \mathbb{N}]/(x_i^2 - x_i \mid i \in \mathbb{N})$. L'ideale $(x_i \mid i \in \mathbb{N})$ non è finitamente generato, e A non è noetheriano. Inoltre, poiché A ha caratteristica 2, l'elevamento al quadrato è un omomorfismo, e tutte le variabili x_i sono idempotenti in A. Quindi tutti gli elementi di A sono idempotenti, ovvero A è un anello *booleano*. Si verifica facilmente che la localizzazione di

un anello booleano è ancora booleano, quindi le localizzazioni $A_{\mathfrak{p}}$ sono anelli booleani locali. Infine, osserviamo che, se B è un anello booleano locale, B ha solo due elementi (ovvero è isomorfo a $\mathbb{Z}/(2)$). Infatti, in un anello locale gli unici idempotenti sono 0 e 1: se così non fosse, ed $e \in B$ fosse un idempotente non banale, e e $1-e$ sono una coppia di idempotenti ortogonali ($e(1-e)=0$) con somma 1, quindi $B \cong R \times S$, con R, S anelli non banali. Se I è un ideale massimale di R e J un ideale massimale di S, allora $I \times S$ e $R \times J$ sono due ideali massimali distinti di B, contraddicendo il fatto che B è locale. D'altra parte tutti gli elementi di B sono idempotenti, per definizione di booleano. Ne segue che 0 e 1 sono gli unici elementi di B. Tornando all'esempio, essendo le localizzazioni $A_{\mathfrak{p}}$ anelli booleani locali, hanno solo due elementi, e quindi sono noetheriani.

6 Moduli noetheriani e artiniani

Definizione. Sia $(\Sigma, <)$ un insieme parzialmente ordinato.

- Σ verifica la **condizione della catena ascendente** (in inglese *ascending chain condition*, o a.c.c.) se ogni catena ascendente $s_1 \leq s_2 \leq \cdots$ stabilizza, cioè $\exists n : s_i = s_n \ \forall i \geq n$.
- Σ verifica la **condizione della catena discendente** (in inglese *descending chain condition*, o d.c.c.) se ogni catena discendente $s_1 \geq s_2 \geq \cdots$ stabilizza.

Definizione (Modulo noetheriano/artiniano)**.** Sia M un A-modulo.

- M si dice **noetheriano** se l'insieme $(\Sigma, \subseteq)$ dei sottomoduli di M, ordinati dall'inclusione, soddisfa la a.c.c..
- M si dice **artiniano** se $(\Sigma, \subseteq)$ soddisfa la d.c.c..

Diciamo anche che un anello A è noetheriano se è un A-modulo noetheriano, ovvero se ogni catena ascendente di ideali di A stabilizza, e che è artiniano se è un A-modulo artiniano, ovvero se ogni catena discendente di ideali di A stabilizza.

Esempio.
- *L'anello dei polinomi $K[x_1, ..., x_n]$ è noetheriano (l'abbiamo dimostrato con le basi di Gröbner*[11]*), ma non è artiniano: infatti la catena discendente $(x_1) \supseteq (x_1^2) \supseteq (x_1^3) \supseteq \cdots$ non è stazionaria.*
- *$\mathbb{Z}$ è noetheriano, in quanto è un PID, ma non artiniano: un controesempio è dato dalla catena $(2) \supseteq (4) \supseteq (8) \supseteq \cdots$.*
- *$\mathbb{R}[x]/(x^2 + 4)$ è noetheriano e artiniano: è infatti un campo, isomorfo a $\mathbb{C}$, e i campi, avendo un numero finito di ideali, sono sia noetheriani che artiniani.*
- *$K[x_i \mid i \in \mathbb{N}]$ non è né noetheriano né artiniano: le catene $(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$ (ascendente) e $(x_1) \supseteq (x_1^2) \supseteq (x_1^3) \supseteq \cdots$ (discendente) non sono stazionarie.*
- *$\mathbb{Z}/(n)$ è sia noetheriano che artiniano, in quanto è un anello finito, e i suoi ideali sono quindi in numero finito.*

Osservazione. Sia $(\Sigma, <)$ un insieme parzialmente ordinato. Allora la a.c.c. equivale al fatto che ogni sottoinsieme non vuoto di Σ ha un elemento massimale. Infatti, se Σ soddisfa la a.c.c., e $F \subseteq \Sigma$, essendo F non vuoto esiste $s_1 \in F$. Se s_1 è massimale in F, abbiamo finito, altrimenti $\exists s_2 \in F : s_2 > s_1$. Se s_2 è massimale in F, abbiamo finito, altrimenti $\exists s_3 \in F : s_3 > s_2$. Possiamo così generare una catena $s_1 < s_2 < \cdots$, che stabilizza per ipotesi in un certo s_α, quindi s_α è

[11] Abbiamo dimostrato in realtà che ogni ideale è finitamente generato, ma vedremo a breve che questo è equivalente alla a.c.c..

massimale in F. Viceversa, se $s_1 < s_2 < \cdots$ è una catena in Σ, è anche un suo sottoinsieme non vuoto. Per ipotesi ammette un elemento massimale s_α, e a quel punto la catena diventa stazionaria.

Di conseguenza, M è noetheriano se e solo se ogni famiglia non vuota di ideali (o sottomoduli) di un anello (o modulo) ammette un elemento massimale, mentre M è artiniano se e solo se ogni famiglia non vuota di ideali (o sottomoduli) di un anello (o modulo) ammette un elemento minimale.

Proposizione 6.1. Sia M un A-modulo. Allora M è noetheriano se e solo se ogni sottomodulo di N è finitamente generato.

Dimostrazione. ($\implies$) Sia $N \subseteq M$, e sia Σ la famiglia dei sottomoduli di N finitamente generati. Notiamo che Σ è non vuoto, in quanto contiene 0. Poiché M è noetheriano, $\exists N_0 \in \Sigma$ massimale. Se per assurdo $N_0 \subsetneq N$, esiste $n \in N \setminus N_0$. Ma allora $N_0 \subsetneq N_0 + \langle n \rangle$, e inoltre $N_0 + \langle n \rangle$ è f.g. in quanto N_0 lo è, contraddicendo la massimalità di N_0. Quindi $N_0 = N \in \Sigma$, cioè N è finitamente generato.

($\impliedby$) Sia $N_0 \subseteq N_1 \subseteq \cdots$ una catena di sottomoduli di M. Allora $\bigcup_i N_i$ è un sottomodulo di N, che è finitamente generato per ipotesi. Se $x_1, ..., x_r$ generano $\bigcup_i N_i$, in particolare $x_i \in N_{k_i}$ per qualche k_i. Ponendo $k = \max_{1 \leq i \leq r} k_i$, abbiamo che N_k contiene tutti i generatori di $\bigcup_i N_i$, quindi sono uguali e la catena stabilizza.

□

Vediamo alcune proprietà dei moduli noetheriani e artiniani.

Proposizione 6.2. Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ una successione esatta. Allora N è noetheriano (o artiniano) se e solo se M, P sono noetheriani (o artiniani).

Dimostrazione. Dimostriamo la proposizione per moduli artiniani, la dimostrazione per quelli noetheriani è analoga.

($\implies$) Supponiamo che N sia artiniano. Se $M_0 \supseteq M_1 \supseteq \cdots$ è una catena discendente di sottomoduli di M, $f(M_0) \supseteq f(M_1) \supseteq \cdots$ è una catena discendente di sottomoduli di N, che stabilizza in quanto N è artiniano. Allora $\exists n \in \mathbb{N} : f(M_m) = f(M_n)$ per ogni $m \geq n$, ed essendo f iniettiva $M_m = M_n$ per ogni $m \geq n$, ovvero la catena degli M_i stabilizza.
Se invece $P_0 \supseteq P_1 \supseteq \cdots$ è una catena discendente in P, $g^{-1}(P_0) \supseteq g^{-1}(P_1) \supseteq \cdots$ è una catena discendente in N, quindi stabilizza, ed esiste $n \in \mathbb{N}$ tale che $g^{-1}(P_m) = g^{-1}(P_n)$ $\forall m \geq n$. Siccome g è surgettiva, $g(g^{-1}(P_i)) = P_i$ $\forall i$, e quindi anche $P_m = P_n$ $\forall m \geq n$, e la catena dei P_i stabilizza.

($\impliedby$) Sia $N_0 \supseteq N_1 \supseteq \cdots$ una catena discendente di sottomoduli di N. Allora $\{f^{-1}(N_i)\}$, $\{g(N_i)\}$ sono catene discendenti in M e in P rispettivamente. Poiché M e P sono artiniani, tali catene sono stazionarie. Inoltre la successione $0 \to f^{-1}(N_i) \to N_i \to g(N_i) \to 0$ è esatta, dove le mappe sono le restrizioni di f a $f^{-1}(N_i)$ e di g a N_i. Infatti $\tilde{f} = f|_{f^{-1}(N_i)}$ è iniettiva (restrizione di iniettiva), $\tilde{g} = g|_{N_i}$ è surgettiva su $g(N_i)$, $\tilde{g} \circ \tilde{f} = 0$ poiché è la restrizione a $f^{-1}(N_i)$ di

$g \circ f = 0$. Infine, se $n \in \ker g|_{N_i} = N_i \cap \ker g,\ g(n) = 0$, quindi $n = f(m)$ per qualche $m \in M$, e $n \in N_i \implies m \in f^{-1}(N_i)$, dunque $n \in \operatorname{Im} f|_{f^{-1}(N_i)}$. Sia $n \in \mathbb{N}$ tale che le catene $\{f^{-1}(N_i)\},\ \{g(N_i)\}$ sono stazionarie da n in poi. Per $m \geq n$, consideriamo il seguente diagramma:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & f^{-1}(N_m) & \longrightarrow & N_m & \longrightarrow & g(N_m) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & f^{-1}(N_n) & \longrightarrow & N_n & \longrightarrow & g(N_n) & \longrightarrow & 0 \end{array}$$

Le due mappe verticali esterne sono l'identità (ricordando che $f^{-1}(N_m) = f^{-1}(N_n),\ g(N_m) = g(N_n)$), e la mappa verticale centrale è un'inclusione, in quanto $N_m \subseteq N_n$. Il diagramma commuta, quindi per il lemma del serpente l'inclusione centrale è un isomorfismo, ovvero $N_n = N_m$ per ogni $m \geq n$, dunque la catena degli N_i stabilizza e N è artiniano.

□

In particolare, sottomoduli e quozienti di moduli noetheriani/artiniani sono ancora noetheriani/artiniani. Sfruttando la successione esatta

$$0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$$

otteniamo che M è noetheriano (o artiniano) se e solo se M_1 ed M_2 lo sono. Induttivamente, si ottiene che una somma diretta finita di moduli è noetheriana/artiniana se e solo se ciascun addendo diretto lo è.

Se A è un anello noetheriano ed M è un A-modulo, allora M è noetheriano se e solo se è finitamente generato. Infatti, ogni modulo noetheriano è ovviamente f.g.. Viceversa, se M è finitamente generato, è un quoziente di A^n per qualche $n \in \mathbb{N}$. Poiché A è un anello noetheriano, A^n è un A-modulo noetheriano, e anche M lo è, dato che è quoziente di un noetheriano.

Se A è un anello, S un sistema moltiplicativo di A e M un A-modulo noetheriano, allora $S^{-1}M$ è un $S^{-1}A$-modulo noetheriano. Questo è vero perché, similmente al caso degli ideali, anche i sottomoduli di $S^{-1}M$ sono della forma $S^{-1}N$, con N un sottomodulo di M. Poiché N è finitamente generato e le immagini dei generatori di N tramite σ_S generano $S^{-1}N$, allora $S^{-1}M$ ha tutti i sottomoduli f.g., cioè è noetheriano.

Se M è un A-modulo noetheriano e $I \subseteq \operatorname{Ann}(M)$ un ideale di A, M è un A/I-modulo noetheriano: infatti, se $N \subseteq M$, N è finitamente generato da $x_1, ..., x_r$. Ma allora, preso $n \in N,\ n = \sum a_i x_i$, si ha anche $n = \sum \overline{a_i} x_i$.

Il prossimo teorema è molto importante, e generalizza un risultato già visto per $K[x_1, ..., x_n]$.

Teorema 6.3 (Teorema della base di Hilbert)**.** Un anello A è noetheriano se e solo se $A[x]$ è noetheriano.

Da questo si ottiene induttivamente che anche $A[x_1, ..., x_n]$ è noetheriano.

Dimostrazione. Un'implicazione è immediata, notando che $A \cong A[x]/(x)$. Per l'implicazione opposta, supponiamo per assurdo che I sia un ideale di $A[x]$ non finitamente generato. In particolare $I \neq 0$, quindi prendiamo $f_1 \in I \setminus (0)$ di grado minimo, poi $f_2 \in I \setminus (f_1)$ di grado minimo, $f_3 \in I \setminus (f_1, f_2)$ di grado minimo, e così via. Ciascun f_i esiste in quanto I non è finitamente generato. Poniamo anche $d_h = \deg f_h \ \forall h$. Osserviamo che i d_h sono una sequenza di numeri naturali debolmente crescente: altrimenti, se $d_h < d_{h+1},\ f_{h+1} \in I \setminus (f_1, ..., f_h) \subseteq I \setminus (f_1, ..., f_{h-1})$, e non avremmo scelto f_h di grado minimo. Per ogni h sia ora $a_h \in A$ il coefficiente di testa di f_h. Otteniamo così una catena ascendente $(a_1) \subseteq (a_1, a_2) \subseteq \cdots$ di ideali di A. Poiché A è noetheriano, la catena stabilizza in $(a_1, ..., a_k)$ per qualche $k \in \mathbb{N}$. In particolare $(a_1, ..., a_k) = (a_1, ..., a_{k+1})$, ossia $a_{k+1} = \sum_{i=1}^{k} b_i a_i$. Vogliamo ora costruire un polinomio $g \in I \setminus (f_1, ..., f_k)$ di grado minore di d_{k+1}. A tale scopo, partiamo da f_{k+1}, e vi sottraiamo dei multipli appropriati degli f_i per cancellare il termine di testa di f_{k+1}. Se $a_i x^{d_i}$ è il termine di testa di f_i, moltiplicando per $b_i x^{d_{k+1}-d_i}$ otteniamo $b_i a_i x^{d_{k+1}}$. Definiamo allora

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

Poiché il termine di testa di f_{k+1} è $a_{k+1}x^{d_{k+1}}$, per costruzione e per la relazione su a_{k+1} il termine di grado $x^{d_{k+1}}$ di g è nullo, quindi $\deg g < d_{k+1}$. Inoltre $g \in I \setminus (f_1, ..., f_k)$, in quanto ovviamente $g \in I$, e $f_{k+1} \notin (f_1, ..., f_k)$. Abbiamo dunque trovato $g \in I \setminus (f_1, ..., f_k)$ di grado minore di d_{k+1}, assurdo per la minimalità di d_{k+1}.

□

6.1 Decomposizione primaria

Vogliamo studiare il problema della *decomponibilità* degli ideali, ovvero capire quando un ideale si può scrivere come intersezione finita di ideali primari. Vedremo che in un anello noetheriano tutti gli ideali sono decomponibili e che i primi minimali contenenti un dato ideale I sono in numero finito.

Esempio. *Sia $I = (x^2, xy) \subseteq K[x, y]$. Poiché l'ideale è monomiale, abbiamo che $(x^2, xy) = (x) \cap (x^2, y)$, che sono due ideali primari: infatti (x) è primo, e (x^2, y) ha radicale massimale (x, y). Questa è una decomposizione primaria di I. Ma abbiamo anche $(x) \cap (x, y)^2 = (x) \cap (x^2, xy, y^2) = (x^2, xy)$, e anche $(x, y)^2$ è primario. Dunque la decomposizione primaria di un ideale, se esiste, non è unica.*

Definizione (Ideale decomponibile)**.** Sia A un anello. Un ideale $I \subseteq A$ si dice **decomponibile** se $\exists q_1, ..., q_r$ ideali primari di A tali che $I = \bigcap_{i=1}^{r} q_i$.

Gli ideali q_i che compaiono nella decomposizione di I si dicono **componenti primarie** di I. Poiché q_i è primario, $\mathfrak{p}_i = \sqrt{q_i}$ è un ideale primo: l'insieme di

tali $\mathfrak{p}_i$ è noto come l'insieme dei **primi associati** di I, denotato con $\mathrm{Ass}(I)$. All'interno di $\mathrm{Ass}(I)$ si distinguono due classi di primi associati: i primi *minimali* (cioè gli elementi di $\mathrm{Ass}(I)$ minimali per inclusione) e i primi *immersi* [12] (tutti gli altri).

Teorema 6.4 (1° teorema di finitezza noetheriana)**.** Se A è un anello noetheriano e I è un ideale di A, allora $\exists h \in \mathbb{N} : (\sqrt{I})^h \subseteq I$.

Dimostrazione. Essendo A noetheriano, $\sqrt{I}$ è finitamente generato da $f_1, ..., f_r$, e per definizione di radicale esistono $h_1, ..., h_r \in \mathbb{N}$ tali che $f_i^{h_i} \in I$. Posto $h = \sum_{i=1}^{r} h_i$, si ha che $f_1^{k_1} \cdots f_r^{k_r} \in I$ per ogni $k_1, ..., k_r$ tali che $k_1 + \cdots + k_r = h$: infatti, per qualche i $k_i \geq h_i$, altrimenti $k_1 + \cdots + k_r < h$. Dunque $(\sqrt{I})^h \subseteq I$. □

Una conseguenza interessante di questo teorema è che, in un anello noetheriano A, il nilradicale è un ideale nilpotente, ovvero esiste $h \in \mathbb{N}$ tale che $\mathcal{N}(A)^h = 0$ (basta applicare il teorema all'ideale 0).

Teorema 6.5. Sia A un anello noetheriano.

1. Se I è irriducibile, allora I è primario.
2. Ogni ideale I è intersezione finita di ideali irriducibili.

Le due affermazioni nel teorema implicano immediatamente che I è decomponibile.

Dimostrazione. 1. Sia I un ideale non primario, e dimostriamo che è riducibile. Dato che I non è primario, $\exists a, b \in A : ab \in I,\ a \notin \sqrt{I},\ b \notin I$. Quindi $a^n \notin I\ \forall n \in \mathbb{N}$. Consideriamo la catena di ideali

$$I \subseteq I : (a) \subseteq I : (a^2) \subseteq I : (a^3) \subseteq \cdots .$$

Per la noetherianità di A, tale catena stabilizza, ovvero esiste $n \in \mathbb{N}$ tale che $I : (a^n) = I : (a^{n+1})$. Dimostriamo ora che

$$I = (I, a^n) \cap (I, b).$$

L'inclusione $\subseteq$ è ovvia; per l'altra, prendiamo $c \in (I, a^n) \cap (I, b)$. Allora $c = da^n + i$, con $d \in A,\ i \in I$. Moltiplicando per a otteniamo che $ac = da^{n+1} + ai \in (aI, ab) \subseteq I$ in quanto $ab \in I$. Chiaramente $ai \in I$, dunque $da^{n+1} \in I$, e quindi $d \in I : (a^{n+1}) = I : a^n$. Si ha allora $da^n \in I \implies c = da^n + i \in I$, come voluto. Usando il fatto che $a^n, b \notin I$, abbiamo $(I, a^n), (I, b) \supsetneq I$, e quindi I è riducibile.

[12] I primi immersi, a dispetto del nome, sono quelli "più grandi", nel senso che contengono un primo minimale. Il nome deriva dalla geometria algebrica: se $P_1, P_2 \in \mathrm{Ass}(I)$ con $P_1 \subseteq P_2,\ P_2$ è un primo immerso, e passando alle varietà associate le inclusioni si rovesciano, ovvero $\mathbb{V}(P_2)$ è "immersa" in $\mathbb{V}(P_1)$.

2. Per assurdo, supponiamo che la famiglia Σ degli ideali di A che non sono intersezione finita di irriducibili sia non vuota. Poiché A è noetheriano, Σ ammette un elemento massimale J. Essendo $J \in \Sigma$, in particolare J è riducibile, e si scrive come $J_1 \cap J_2$, con $J \subsetneq J_1, J_2$. Per la massimalità di J in Σ, $J_1, J_2 \notin \Sigma$, quindi $J_i = \bigcap_{h=1}^{r_i} Q_h^{(i)}$, con i $Q_h^{(i)}$ irriducibili. Ma allora $J = \bigcap_{i=1}^{2} \bigcap_{h=1}^{r_i} Q_h^{(i)}$ è intersezione finita di irriducibili, assurdo.

□

Sia I un ideale decomponibile, con decomposizione primaria $I = \bigcap_{i=1}^{h} q_h$. Vogliamo estrarre una decomposizione primaria *minimale*, in questo modo:

- $q_j \not\supseteq \bigcap_{i \neq j} q_i$: altrimenti non influirebbe sull'intersezione;
- a ciascun q_i corrisponde un unico primo associato $\mathfrak{p}_i$.

La seconda condizione si può soddisfare in virtù del seguente lemma:

Lemma 6.6. Siano q_1, q_2 due ideali $\mathfrak{p}$-primari (ovvero ideali primari con radicale $\mathfrak{p}$). Allora $q_1 \cap q_2$ è ancora $\mathfrak{p}$-primario.

Dimostrazione. $\sqrt{q_1 \cap q_2} = \sqrt{q_1} \cap \sqrt{q_2} = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$, quindi, una volta mostrato che $q_1 \cap q_2$ è primario, sarà chiaramente $\mathfrak{p}$-primario. Siano $a, b \in A : ab \in q_1 \cap q_2,\ a \notin q_1 \cap q_2$. Se $a \notin q_1$, poiché q_2 è primario, $b \in \sqrt{q_1} = \mathfrak{p} = \sqrt{q_1 \cap q_2}$. Se $a \notin q_2$, lo stesso argomento funziona, scambiando q_1 con q_2.

□

Alla luce di questo lemma, possiamo accorpare tutti i q_i con lo stesso radicale in un unico ideale primario, intersecandoli tutti.

Possiamo immaginare la decomposizione primaria di un ideale come composta di due "pezzi":

$$I = q_1 \cap \cdots \cap q_t \cap q_{t+1} \cap \cdots \cap q_r,$$

dove i primi associati $\mathfrak{p}_1, ..., \mathfrak{p}_t$ sono minimali, e $\mathfrak{p}_{t+1}, ..., \mathfrak{p}_r$ sono immersi.

Vogliamo giungere a due risultati di unicità: l'indipendenza di $\mathrm{Ass}(I)$ dalla decomposizione primaria di I e l'unicità dei q_i corrispondenti ai primi associati minimali.

Lemma 6.7. Sia q un ideale $\mathfrak{p}$-primario, e $a \in A$. Allora:

- se $a \in q,\ q : a = (1)$;
- se $a \notin q,\ q : a$ è un ideale $\mathfrak{p}$-primario;
- se $a \notin p,\ q : a = q$.

Dimostrazione. Ovviamente $q : a = (1)$ se $a \in q$. Supponiamo che $a \notin q$, e osserviamo che $q : a \subseteq \mathfrak{p}$, in quanto, se $b \in q : a,\ ab \in q$, ed essendo $a \notin q$ e q primario, $b \in \sqrt{q} = \mathfrak{p}$. Abbiamo dunque $q \subseteq q : a \subseteq \mathfrak{p}$, e passando ai radicali $\mathfrak{p} \subseteq \sqrt{q : a} \subseteq \mathfrak{p}$, ovvero $\sqrt{q : a} = \mathfrak{p}$. Resta da dimostrare che $q : a$ è primario. Sia $bc \in q : a$, con $b \notin \mathfrak{p}$. Allora $abc \in q$, e $ac \in q$ per la primarietà di q, quindi $c \in q : a$. Infine, se $a \notin \mathfrak{p}$, e $b \in q : a$, allora $ab \in q$ e dunque $b \in q$, e si ha che $q = q : a$ (l'altro contenimento è banale).

□

Teorema 6.8 (1° teorema di unicità)**.** Sia I un ideale decomponibile. Allora

$$\mathrm{Ass}(I) = \{\sqrt{I : a} \mid a \in A : \sqrt{I : a} \text{ è primo}\}.$$

Osserviamo che questa scrittura di $\mathrm{Ass}(I)$ non dipende da nessuna decomposizione primaria particolare di I, ma solo dall'ideale I stesso.

Dimostrazione. ($\supseteq$) Sia $I = \bigcap q_i$ una decomposizione primaria minimale di I, e sia $a \in A$. Allora abbiamo $\sqrt{I : a} = \sqrt{\bigcap q_i : a} = \sqrt{\bigcap (q_i : a)} = \bigcap \sqrt{q_i : a}$. Se $a \in I$, $\sqrt{I : a} = (1)$, che non è primo. Assumiamo quindi $a \notin I$ e $\sqrt{I : a}$ primo. Dal lemma precedente sappiamo che $q_i : a \neq (1)$ se e solo se $a \notin q_i$, e in tal caso $q_i : a$ è $\mathfrak{p}_i$-primario. Dunque vale che $\sqrt{I : a} = \bigcap \sqrt{q_i : a} = \bigcap\limits_{i : a \notin q_i} \mathfrak{p}_i$. Poiché $\sqrt{I : a}$ è primo, deve allora essere uguale a uno dei $\mathfrak{p}_i$ dell'intersezione, cioè per qualche i $\sqrt{I : a} = \mathfrak{p}_i \in \mathrm{Ass}(I)$.

($\subseteq$) Sia $\mathfrak{p}_i = \sqrt{q_i} \in \mathrm{Ass}(I)$. Per la minimalità della decomposizione, esiste $a \in \bigcap\limits_{j \neq i} q_j \setminus q_i$. Ma allora $\sqrt{I : a} = \bigcap\limits_{h : a \notin q_h} \mathfrak{p}_h = \mathfrak{p}_i$, che conclude la dimostrazione.

□

Abbiamo dunque che, se I è un ideale decomponibile, poiché $\mathrm{Ass}(I)$ è indipendente dalla decomposizione primaria di I, e per ogni decomposizione c'è un numero finito di primi associati, allora $\mathrm{Ass}(I)$ è un insieme finito. In particolare, se A è noetheriano, $\mathrm{Ass}(I)$ è finito per ogni I, essendo ogni ideale di A decomponibile (*3° teorema di finitezza noetheriana*[13]).

Sia A un anello nel quale l'ideale 0 sia decomponibile, e sia $0 = \bigcap q_i$. Sappiamo già che $\mathcal{D}(A) = \bigcup\limits_{a \neq 0} \sqrt{0 : a}$. Mostriamo che $\mathcal{D}(A) = \bigcup\limits_{\mathfrak{p} \in \mathrm{Ass}(0)} \mathfrak{p}$. Se $\mathfrak{p} \in \mathrm{Ass}(0)$, per il teorema di unicità esiste $a \neq 0$ tale che $\sqrt{0 : a} = \mathfrak{p}$. Viceversa, se $a \in \mathcal{D}(A) \setminus \{0\}$, $a \notin (0) = \bigcap q_i$, quindi $a \notin q_i$ per qualche i, e $\sqrt{0 : a} = \bigcap\limits_{i : a \notin q_i} \mathfrak{p}_i \subseteq \mathfrak{p}_i \in \mathrm{Ass}(0)$.

Lemma 6.9. Sia A un anello, q un ideale $\mathfrak{p}$-primario di A, ed S un sistema moltiplicativo di A. Allora:

- se $S \cap \mathfrak{p} \neq \emptyset$, allora $S^{-1}q = (1)$;

[13] Il 3° teorema di finitezza completo afferma che, se M è un A-modulo finitamente generato con A noetheriano, allora $\mathrm{Ass}(M)$ è finito, dove $\mathrm{Ass}(M)$ è l'insieme dei primi di A che sono annullatori di qualche elemento di M, e generalizza $\mathrm{Ass}(I)$ per I ideale di A.

- se $S \cap \mathfrak{p} = \emptyset$, allora $S^{-1}q$ è un ideale $S^{-1}\mathfrak{p}$-primario di $S^{-1}A$, e $(S^{-1}q)^c = q$.

Dimostrazione. Ricordando che localizzazione e radicale commutano, abbiamo $\sqrt{S^{-1}q} = S^{-1}\sqrt{q} = S^{-1}\mathfrak{p}$, che è (1) se $S \cap \mathfrak{p} \neq \emptyset$, ed è un ideale primo se $S \cap \mathfrak{p} = \emptyset$.

Concentriamoci sul caso $S \cap \mathfrak{p} = \emptyset$. Mostriamo che $S^{-1}q$ è un ideale primario (già sappiamo che il suo radicale è $S^{-1}\mathfrak{p}$): siano $\frac{a}{s}, \frac{b}{t} : \frac{ab}{st} \in S^{-1}q$ e $\frac{a}{s} \notin S^{-1}q$. Osserviamo che $aw \notin q \ \forall w \in S$. Si ha $\frac{ab}{st} = \frac{c}{u}$ con $c \in q$, e quindi $\exists v \in S : abuv = cstv \in q$. Per quanto appena osservato $auv \notin q$, e per la primarietà di q deve essere $b \in \mathfrak{p}$, e dunque $\frac{b}{t} \in S^{-1}\mathfrak{p}$. Per l'ultima affermazione, sappiamo che $(S^{-1}q)^c = q^{ec} = \bigcup_{s \in S} q : s$. Ovviamente $q^{ec} \supseteq q$; d'altro canto, se $a \in q^{ec}$ ed $s \in S$ è tale che $as \in q$, poiché $S \cap \mathfrak{p} = \emptyset,\ s \notin \mathfrak{p}$ e dunque $a \in q$.

□

Teorema 6.10 (2° teorema di unicità)**.** Sia I un ideale decomponibile. Allora le componenti primarie relative ai primi minimali sono univocamente determinate.

Dimostrazione. Sia $\mathfrak{p}_i \in \mathrm{Ass}(I)$ minimale, e poniamo $Q_i = (IA_{\mathfrak{p}_i})^c$ (dove $IA_{\mathfrak{p}_i} = S_i^{-1}I$, con $S_i = A \setminus \mathfrak{p}_i$). Se $I = \bigcap q_j$ è una decomposizione primaria di I, allora $IA_{\mathfrak{p}_i} = (\bigcap q_j)A_{\mathfrak{p}_i} = \bigcap q_j A_{\mathfrak{p}_i}$, e per il lemma precedente $q_j A_{\mathfrak{p}_i} \neq (1) \iff S_i \cap \mathfrak{p}_j = \emptyset \iff \mathfrak{p}_j \subseteq \mathfrak{p}_i$. Ma $\mathfrak{p}_i$ è minimale in $\mathrm{Ass}(I)$, quindi $\mathfrak{p}_j = \mathfrak{p}_i$. Si deduce che $IA_{\mathfrak{p}_i} = \bigcap q_j A_{\mathfrak{p}_i} = q_i A_{\mathfrak{p}_i}$, e se contraiamo entrambi i membri, ancora per il lemma precedente $(q_i A_{\mathfrak{p}_i})^c = (S_i^{-1}q_i)^c = q_i$, da cui si ha $Q_i = (IA_{\mathfrak{p}_i})^c = (q_i A_{\mathfrak{p}_i})^c = q_i$. Dato che Q_i non dipende dalla decomposizione primaria, ma solo da I, si ha la tesi.

□

Concludiamo la discussione parlando dei primi minimali. In particolare, mostriamo che i primi minimali di A che contengono I (che abbiamo indicato con $\mathrm{Min}(I)$ all'inizio) coincidono con gli elementi minimali di $\mathrm{Ass}(I)$ se I è decomponibile.

- Se $\mathfrak{p} \in \mathrm{Min}(I)$, sappiamo che $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}$. Essendo I decomponibile, se $I = \bigcap q_i$ è una decomposizione primaria di I, $\sqrt{I} = \bigcap \mathfrak{p}_i$, dove i $\mathfrak{p}_i$ sono gli elementi minimali di $\mathrm{Ass}(I)$. Dato che $\bigcap \mathfrak{p}_i = \sqrt{I} \subseteq \mathfrak{p}$, poiché $\mathfrak{p}$ è primo esso deve contenere uno dei $\mathfrak{p}_i$. Ma per la minimalità di $\mathfrak{p}$ in $\mathrm{Spec}\, A$ si deve avere $\mathfrak{p} = \mathfrak{p}_i$. Dunque, se $\mathfrak{p} \in \mathrm{Min}(I)$ allora $\mathfrak{p}$ deve essere un primo associato minimale di I. Questo dimostra che $\mathrm{Min}(I)$ è un insieme finito, in quanto sottoinsieme di $\mathrm{Ass}(I)$ che è finito.

- Viceversa, sia $\mathfrak{p}_i$ minimale in $\mathrm{Ass}(I)$. Prendiamo $\mathfrak{p} \in \mathrm{Min}(I)$ tale che $I \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$; poiché $\mathfrak{p}$ è primo e $I = \bigcap_{j=1}^{k} \mathfrak{p}_j$, allora $\mathfrak{p}$ contiene un qualche $\mathfrak{p}_j$ minimale in $\mathrm{Ass}(I)$. Ma anche $\mathfrak{p}_i$ è minimale in $\mathrm{Ass}(I)$, quindi $\mathfrak{p}_j = \mathfrak{p} = \mathfrak{p}_i$ e $\mathfrak{p}_i \in \mathrm{Min}(I)$.

Da questo discende che $\mathrm{Min}(I)$ è finito se I è un ideale decomponibile. Quindi, se A è noetheriano, $\mathrm{Min}(I)$ è finito per ogni ideale I di A: questo è il *2° teorema di finitezza noetheriana.*

6.2 Anelli artiniani

Ricordiamo che un anello A è artiniano se è artiniano come A-modulo, ovvero se le catene discendenti di ideali stabilizzano, o equivalentemente se ogni famiglia non vuota di ideali ammette un elemento minimale. Vogliamo caratterizzare gli anelli artiniani, e nel farlo giungeremo anche a un teorema di struttura.

Proposizione 6.11 (Proprietà degli anelli artiniani)**.** Sia A un anello artiniano. Allora:

1. $\mathrm{Spec}\, A = \mathrm{Max}\ A$, ovvero A è 0-dimensionale;
2. $\mathrm{Spec}\, A$ è finito;
3. il nilradicale di A è nilpotente: $\exists n \in \mathbb{N} : \mathcal{N}(A)^n = (0)$.

Dimostrazione. 1. Sia $\mathfrak{p} \in \mathrm{Spec}\, A$. Allora $A/\mathfrak{p}$ è un dominio artiniano, e vogliamo mostrare che è un campo. Sia dunque $\overline{a} \in A/\mathfrak{p} \setminus (\overline{0})$. Poiché $A/\mathfrak{p}$ è artiniano, la catena di ideali $(\overline{a}) \supseteq (\overline{a}^2) \supseteq (\overline{a}^3) \supseteq \cdots$ stabilizza, ed esiste $n \in \mathbb{N}$ tale che $(\overline{a}^n) = (\overline{a}^{n+1})$. Possiamo dunque scrivere $\overline{a}^n = \overline{b}\overline{a}^{n+1}$ per qualche $b \in A/\mathfrak{p}$. Poiché $A/\mathfrak{p}$ è un dominio e $\overline{a} \neq \overline{0}$, deve essere $\overline{b}\overline{a} = \overline{1}$, quindi $\overline{a}$ è invertibile, $A/\mathfrak{p}$ è un campo e $\mathfrak{p}$ è massimale.

2. Supponiamo per assurdo che A possieda infiniti ideali primi. Per quanto appena dimostrato essi sono anche massimali. Sia dunque $\{\mathfrak{m}_i\}_{i\in\mathbb{N}}$ un insieme infinito di ideali massimali distinti di A. La catena discendente di ideali
$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supseteq \cdots$$
è stazionaria, essendo A artiniano, quindi esiste $n \in \mathbb{N}$ tale che $\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_{n+1} \subseteq \mathfrak{m}_{n+1}$. Poiché $\mathfrak{m}_{n+1}$ è primo, deve contenere qualche $\mathfrak{m}_i$, e siccome $\mathfrak{m}_i$ è massimale, $\mathfrak{m}_i = \mathfrak{m}_{n+1}$, che contraddice l'ipotesi che gli $\mathfrak{m}_i$ fossero distinti; dunque i massimali (e anche i primi) di A sono in numero finito.

3. La catena discendente di ideali
$$\mathcal{N}(A) \supseteq \mathcal{N}(A)^2 \supseteq \mathcal{N}(A)^3 \supseteq \cdots$$
è stazionaria, quindi $\mathcal{N}(A)^n = \mathcal{N}(A)^{n+1}$ per qualche $n \in \mathbb{N}$. Se $\mathcal{N}(A)^n = (0)$, abbiamo finito, quindi supponiamo per assurdo che $\mathcal{N}(A)^n \neq (0)$. Sia $\Sigma = \{I \subseteq A \text{ ideale} \mid I\mathcal{N}(A)^n \neq (0)\}$. Σ è non vuota in quanto $(1) \in \Sigma$ ($\mathcal{N}(A)^n \neq (0)$). Poiché A è artiniano, Σ ammette un elemento minimale J. Dato che $J\mathcal{N}(A)^n \neq (0)$, $\exists a \in J : a\mathcal{N}(A)^n \neq (0)$. Dunque $(a) \in \Sigma$, e $(a) \subseteq J$. Poiché J è minimale in Σ, $J = (a)$. Notiamo anche che

$(a)\mathcal{N}(A)^n \in \Sigma$: infatti, $(a)\mathcal{N}(A)^n \cdot \mathcal{N}(A)^n = (a)\mathcal{N}(A)^{2n} = (a)\mathcal{N}(A)^n \neq (0)$, dove $\mathcal{N}(A)^{2n} = \mathcal{N}(A)^n$ in quanto la catena è stazionaria. Inoltre $(a)\mathcal{N}(A)^n \subseteq (a) = J$, e per minimalità di J $(a)\mathcal{N}(A)^n = (a)$. Quindi possiamo scrivere $a = ab$, con $b \in \mathcal{N}(A)^n \subseteq \mathcal{N}(A)$. Quindi b è nilpotente, e inoltre $a = ab = (ab)b = ab^2 = (ab)b^2 = ab^3$. Iterando si ottiene che $a = ab^k \ \forall k \in \mathbb{N}$. Ma b è nilpotente, quindi per k abbastanza grande $a = ab^k = 0$, e $J = (0)$, che è assurdo in quanto $J\mathcal{N}(A)^n \neq (0)$.

□

Teorema 6.12 (Teorema di struttura per anelli artiniani)**.** *A è un anello artiniano se e solo se è un prodotto diretto finito di anelli artiniani locali.*

Dimostrazione. ($\Longleftarrow$) Segue dalla proposizione sulle somme dirette: se A, B sono anelli artiniani, anche $A \oplus B$ è artiniano. Quindi una somma diretta finita (che è anche un prodotto diretto finito) di anelli artiniani è un anello artiniano.

($\Longrightarrow$) Sia A artiniano. Allora A possiede un numero finito di ideali primi: $\operatorname{Spec} A = \{\mathfrak{m}_1, ..., \mathfrak{m}_h\}$, e tali primi sono tutti massimali. In particolare tutti gli m_i sono a due a due comassimali. Quindi $\mathcal{N}(A) = \bigcap_{i=1}^{h} \mathfrak{m}_h = \prod_{i=1}^{h} \mathfrak{m}_i$. Se $n \in \mathbb{N}$ è tale che $\mathcal{N}(A)^n = (0)$, allora $(0) = \mathcal{N}(A)^n = (\prod_{i=1}^{h} \mathfrak{m}_i)^n = \prod_{i=1}^{h} \mathfrak{m}_i^n$. Inoltre gli ideali $\mathfrak{m}_i^n$ sono ancora a due a due comassimali: infatti un ideale massimale che contiene $\mathfrak{m}_i^n + \mathfrak{m}_j^n$ dovrebbe contenere sia $\mathfrak{m}_i$ che $\mathfrak{m}_j$, ma allora conterrebbe 1, essendo $\mathfrak{m}_i, \mathfrak{m}_j$ massimali distinti. Quindi $\mathfrak{m}_i^n + \mathfrak{m}_j^n = (1)$, dato che non è contenuto in nessun ideale massimale. Per il teorema cinese del resto,

$$A = A/(0) = A/\prod_{i=1}^{h} \mathfrak{m}_i^n \cong \prod_{i=1}^{h} A/\mathfrak{m}_i^n.$$

Ciascun anello $A/\mathfrak{m}_i^n$ è artiniano, in quanto quoziente di artiniano; inoltre un ideale massimale di $A/\mathfrak{m}_i^n$ corrisponde a un massimale di A che contiene $\mathfrak{m}_i^n$, che deve essere dunque $\mathfrak{m}_i$. Abbiamo allora che gli anelli $A/\mathfrak{m}_i^n$ sono locali, con ideale massimale $\overline{\mathfrak{m}_i}$, e A è prodotto diretto finito di anelli artiniani locali.

□

Esempio. *Se I è un ideale 0-dimensionale di $K[x_1, ..., x_n]$, con K un campo algebricamente chiuso, l'anello delle coordinate di $\mathbb{V}(I)$, $A/\sqrt{I}$, è un anello artiniano. Allora avevamo visto che la varietà associata a I è finita, cioè è un'unione di punti, e ciascun punto di K^n corrisponde a un ideale massimale di $K[x_1, ..., x_n]$. Avevamo anche dimostrato che $A/\sqrt{I}$ è una somma diretta di campi, che sono anelli artiniani locali.*

Proposizione 6.13. Sia V uno spazio vettoriale su un campo K. Allora sono equivalenti:

- V ha dimensione finita;
- V è noetheriano;

- V è artiniano.

Dimostrazione. Se V ha dimensione finita, è un K-modulo finitamente generato, e K è sia noetheriano che artiniano, quindi V è noetheriano e artiniano. Se invece V ha dimensione finita, e $\{v_i\}_{i\in I}$ è una base (infinita) di V, se poniamo $U_n = \langle v_i \mid 1 \leq i \leq n\rangle,\ n \in \mathbb{N}$, gli U_n formano una catena ascendente non stazionaria di sottospazi di V, che quindi non è noetheriano. Se poniamo $W_n = \langle v_i \mid i \geq n\rangle,\ n \in \mathbb{N}$, i W_n formano una catena discendente non stazionaria di sottospazi di V, che quindi non è artiniano. □

Lemma 6.14. Sia A un anello e $\mathfrak{m}_1, ...\mathfrak{m}_h$ ideali massimali di A, non necessariamente distinti. Allora $A/\prod_{i=1}^{h} \mathfrak{m}_i$ è artiniano se e solo se è noetheriano. In particolare, se (0) è prodotto di ideali massimali, allora A è artiniano se e solo se A è noetheriano.

Dimostrazione. Procediamo per induzione su h.

Passo base, $h = 1$: in questo caso $A/\mathfrak{m}_1$ è un campo, e quindi è sia artiniano che noetheriano.

Passo induttivo, $h - 1 \implies h$: consideriamo la proiezione

$$\pi : A/\prod_{i=1}^{h} \mathfrak{m}_i \longrightarrow A/\prod_{i=1}^{h-1} \mathfrak{m}_i.$$

Abbiamo che $\ker \pi = \prod_{i=1}^{h-1} \mathfrak{m}_i/\prod_{i=1}^{h} \mathfrak{m}_i$. Osserviamo che $\mathfrak{m}_h \subseteq \mathrm{Ann}(\prod_{i=1}^{h-1} \mathfrak{m}_i/\prod_{i=1}^{h} \mathfrak{m}_i)$, quindi $\prod_{i=1}^{h-1} \mathfrak{m}_i/\prod_{i=1}^{h} \mathfrak{m}_i$ ha una struttura di $A/\mathfrak{m}_h$-modulo. Ma $A/\mathfrak{m}_h$ è un campo, ovvero $\prod_{i=1}^{h-1} \mathfrak{m}_i/\prod_{i=1}^{h} \mathfrak{m}_i$ è uno spazio vettoriale su $A/\mathfrak{m}_h$, e abbiamo mostrato che uno spazio vettoriale è noetheriano se e solo se è artiniano. Consideriamo la successione esatta

$$0 \to \prod_{i=1}^{h-1} \mathfrak{m}_i/\prod_{i=1}^{h} \mathfrak{m}_i \to A/\prod_{i=1}^{h} \mathfrak{m}_i \to \prod_{i=1}^{h-1} \mathfrak{m}_i \to 0.$$

I due moduli laterali sono noetheriani se e solo se sono artiniani (quello a sinistra per quanto appena detto, quello a destra per ipotesi induttiva). Dunque il modulo centrale, $A/\prod_{i=1}^{h} \mathfrak{m}_i$, è noetheriano se e solo se è artiniano. Infine, osserviamo che gli ideali di $A/\prod_{i=1}^{h} \mathfrak{m}_i$ sono anche A-sottomoduli, quindi $A/\prod_{i=1}^{h} \mathfrak{m}_i$ è noetheriano (come anello) se e solo se è artiniano (come anello).

□

Teorema 6.15 (Caratterizzazione degli anelli artiniani)**.** Un anello A è artiniano se e solo se è noetheriano di dimensione 0.

Dimostrazione. ($\Longrightarrow$) Se A è artiniano, ha dimensione 0 in quanto tutti i primi sono massimali. Inoltre il nilradicale di A è nilpotente ed è prodotto di ideali massimali, quindi $(0) = \mathcal{N}(A)^n$ è anch'esso prodotto di ideali massimali. Per il lemma precedente, A è noetheriano.

($\Longleftarrow$) Poiché A è noetheriano, (0) ammette una decomposizione primaria minimale: sia $(0) = \bigcap q_i$, con i q_i primari e $\sqrt{q_i}$ primi distinti. Allora $\mathcal{N}(A) = \sqrt{(0)} = \sqrt{\bigcap q_i} = \bigcap \sqrt{q_i}$. Gli ideali $\sqrt{q_i}$ sono primi, e siccome A è 0-dimensionale, sono anche massimali; dunque $\mathcal{N}(A)$ è un'intersezione finita di ideali massimali, e quindi è un prodotto finito di tali massimali: $(0) = \bigcap \mathfrak{m}_i = \prod \mathfrak{m}_i$, dove $\mathfrak{m}_i = \sqrt{q_i}$. Per il 1° teorema di finitezza, $\mathcal{N}(A)^n = (0) = \prod \mathfrak{m}_i^n$, per qualche $n \in \mathbb{N}$. Abbiamo dunque che (0) è prodotto di ideali massimali nell'anello noetheriano A; per il lemma precedente A è artiniano.

□