Appunti di Algebra2

Luca Bruni
Viola Giovannini

18 settembre 2018

Indice

Introduzione

I seguenti appunti sono tratti dalle lezioni tenute dalla professoressa Gianni Patrizia durante il corso di Algebra2 tenutosi nel secondo semestre dell'anno accademico 2016/2017. Gli enunciati segnati in rosso mancano di pezzi o elementi che devono essere aggiunti. Se non ci sono pezzi rossi allora è tutto bello.

Capitolo 1

Anelli

In questo primo capitolo vengono date le definizioni di base di anello commutativo con identità e mostrati i primi risultati generali. Viene poi affrontato in maniera più approfondita l'anello dei polinomi con particolare attenzione agli ideali monomiali, e altro ancora.

1.1 Anelli, definizioni e prime proprietà

Definizione 1.1 *Una terna* $(A, +, \cdot)$ *tale che*

- $(A, +)$ *è un gruppo abeliano;*
- $(A, \cdot)$ *gode della proprietà associativa ed esiste l'elemento neutro* 1*;*
- $\forall a, b, c \in A, (a + b)c = ac + bc$ *e inoltre* $c(a + b) = ca + bc$ *(proprietà distributiva)*

si dice ***anello****. Se vale la proprietà commutativa per il prodotto, allora l'anello si dice* ***commutativo****.*

Gli anelli considerati hanno la caratteristica che $1 \neq 0$ altrimenti siamo di fronte allo **stupid ring** (anello banale), cioè $A = 0$. Esempi di anelli commutativi sono $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$. In generale $A[x_1, x_2, ..., x_n]$, cioè i polinomi in n variabili a coefficienti in un anello, è un anello. Un esempio di anello non commutativo è $M_n(\mathbb{R})$ cioè le matrici quadrate a coefficienti in $\mathbb{R}$. Gli anelli considerati in tutta la trattazione devono essere considerati commutativi e con identità.

Definizione 1.2 *I seguenti elementi prendono un nome specifico per la loro importanza:*

- $a \in A$ *si dice* ***unità*** *se esiste un elemento* $b \in A$ *tale che* $ab = 1$*. L'insieme delle unità viene indicato con* A^**;*
- $a \in A$ *si dice* ***zero divisore*** *se esiste* $b \neq 0 \in A$ *tale che* $ab = 0$*. L'insieme degli zero divisori si indica con* $\mathcal{D}(A)$*;*
- $a \in A$ *si dice* ***nilpotente*** *se esiste* $n \in \mathbb{N}$ *tale che* $a^n = 0$*. L'insieme dei nilpotenti si indica con* $\mathcal{N}(A)$ *e vale che* $\mathcal{N}(A) \subseteq \mathcal{D}(A)$*;*
- $a \in A$ *si dice* ***idempotente*** *se* $a^2 = a$*.*

Prendiamo per esempio l'anello $\mathbb{Z}_{36}$. In questo caso abbiamo che gli invertibili sono tutti gli m tali che $(m, 36) = 1$, i divisori di zero sono tutti gli elementi a tali che $2|a$ o $3|a$. I nilpotenti sono tutti gli elementi che sono divisibili per 6.

Definizione 1.3 *Un insieme $I \subset A$ tale che I è un gruppo con la somma e $\forall a \in A, \forall x \in I \Rightarrow ax \in I$ si chiama* ***ideale****.*

Prendiamo un sottoinsieme S di A. Indichiamo con (S) l'insieme di tutte le combinazioni lineari a valori in S ovvero $(S) = \{a_1 s_1 + ... + a_n s_n | a_i \in A, s_i \in S\}$. (S) è banalmente un ideale e inoltre, se S è finito, (S) si dice **finitamente generato**. Se $S = \{a\}$ allora l'ideale $(S) = (a)$ si dice **principale**.

Definizione 1.4 *Un anello A in cui tutti i suoi ideali sono principali si dice* ***principal ideal ring*** *(PIR). Se A è anche un dominio, allora si dice che è un* ***principal ideal domain*** *(PID).*

Definizione 1.5 *I seguenti ideali prendono un nome specifico per la loro importanza:*

- *I si dice* ***principale*** *se esiste un elemento $a \in A$ tale che $I = (a)$;*
- *I si dice* ***finitamente generato*** *se esistono $a_1, ..., a_n \in A$ tali che $I = (a_1, ..., a_n)$;*
- *I si dice* ***primo*** *se $ab \in I \Rightarrow a \in I \vee b \in I$. L'insieme degli ideali primi si chiama* ***spettro di*** *A e si indica con $Spec(A)$;*
- *I si dice* ***primario*** *se $ab \in I \Rightarrow a \in I \vee \exists n \in \mathbb{N} | b^n \in I$;*
- *I si dice* ***proprio*** *se $I \subsetneq A$;*
- *I si dice* ***massimale*** *se è proprio e massimale rispetto all'inclusione.*

Teorema 1.1.1 (Lemma di Zorn) *: Sia Ω un insieme non vuoto e parzialmente ordinato (valgono per $\leq$ le proprietà transitiva, riflessiva e antisimmetrica). Definiamo* ***catena*** *C un sottoinsieme di Ω totalmente ordinato. Se ogni catena è superiormente limitata ($\exists b \in \Omega$ t.c. $\forall \delta \in C, \delta \leq b$) allora esiste in Ω almeno un elemento massimale.*

Proposizione 1.1.2 *Sia A un anello non banale. Esiste almeno un ideale massimale.*

Dimostrazione: Sia $\Omega = \{I \subsetneq A$, ideali propri$\}$ ordinati con l'inclusione. Ω è non vuoto poiché $(0) \in \Omega$; prendiamo allora una catena $I_1 \subset I_2 \subset ...$ e definiamo $I = \cup_\alpha I_\alpha$. Si verifica che I è un ideale proprio (basta fare le verifiche nell'ideale più grande). Ma allora ogni catena è superiormente limitata da un opportuno I e quindi, per il lemma di Zorn, esiste un elemento massimale.

⋈

In generale non è vero che l'unione di ideali è un ideale. Nella dimostrazione precedente è cruciale che gli ideali siano uno contenuto nell'altro.

Proposizione 1.1.3 *Sia A anello e $a \notin A^*$. Allora esiste M ideale massimale tale che $a \in M$.*

Dimostrazione: La dimostrazione ricalca passo passo quella precedente considerando $\Omega = \{I \subsetneq A, a \in I\}$. L'insieme è non vuoto poiché contiene (a) e pertanto si procede come sopra.

⋈

Definizione 1.6 *Data una famiglia $\{I_\alpha\}_{\alpha \in H}$ definiamo le seguenti operazioni tra ideali:*

- ***Intersezione:*** *Si agisce come fossero insiemi: $J = \cap_\alpha I_\alpha$. J è un ideale;*
- ***Somma:*** *$J = \sum_\alpha I_\alpha = (\cup_\alpha I_\alpha)$, cioè la somma di ideali è come l'ideale generato dall'unione insiemistica di ideali;*

- ***Prodotto:*** $J = I_1 I_2 \cdots I_n = \{\sum_j i_j^{(1)} i_j^{(2)} \cdots i_j^{(n)}\}$. *Il prodotto è definito solo per famiglie finite di ideali;*
- ***Divisione:*** $I : J = \{a \in A |\ aJ \subseteq I\} = \{a \in A | aj \in I, \forall j \in J\}$. *In particolare l'operazione* $0 : J$ *prende il nome di* ***annullatore*** *di* J *e si indica con* $Ann(J)$. *Chiamiamo* ***colon*** *l'ideale* $I : J$*;*
- ***Radicale:*** $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N} \text{ t.c. } a^n \in I\}$.

Proposizione 1.1.4 *Sia* A *anello e* $I \subseteq A$ *ideale. Allora* $\sqrt{I}$ *è un ideale. In particolare un ideale si dice* ***radicale*** *se* $I = \sqrt{I}$.

Dimostrazione: Verifichiamo prima la proprietà di assorbimento: sia $k \in A$ e $a \in \sqrt{I}$, voglio mostrare che $ka \in \sqrt{I}$. Considero $(ka)^n = k^n a^n \in I$ poiché $a^n \in I$ e I è un ideale. Verifichiamo adesso che $\sqrt{I}$ è chiuso per somma. Siano $a^n, b^m \in I$. Consideriamo

$$(a+b)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} =$$

$$\sum_{k=0}^{n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} + \sum_{k=n}^{n+m-1} \binom{m+n-1}{k} a^k b^{m+n-1-k}$$

Da cui il primo termine della sommatoria appartiene a I poiché è somma di elementi che appartengono ad I (sono tutti multipli di b^m), mentre il secondo termine della sommatoria appartiene a I perché ogni elemento è multiplo di a^n.

$3^2 3$

⋈

Osservazione: $\sqrt{0} = \mathcal{N}(A)$ è pertanto i nilpotenti sono un ideale. L'insieme degli zero divisori, invece, non è detto che sia un ideale (per un controesempio si consideri $\mathbb{Z}_6$).

Proposizione 1.1.5 *Sia* A *anello, allora* $\mathcal{N}(A) = \bigcap_{P \subseteq A} P$ *con* P *ideale primo.*

Dimostrazione: $Nil(A) = \{a \in A \text{ t.c. } \exists n \in \mathbb{N} \text{ t.c. } a^n = 0\}$. Se $a \in \mathcal{N}(A) \Rightarrow a^n \in P$ per ogni P. Essendo P un ideale primo $a^{n-1} a \in P \Rightarrow a \in P$ (per induzione). Quindi $\mathcal{N}(A) \subseteq \bigcap_{P \subset A} P$. Sia adesso $a \notin \mathcal{N}(A)$, voglio dimostrare che esiste P tale che $a \notin P$. Sia $\Omega = \{I \subset A \text{ t.c. } \forall n \in \mathbb{N}, a^n \notin I\}$, voglio dimostrare che P primo è elemento massimale. Consideriamo una catena C: $I_1 \subset I_2 \subset ...$ con $I_i \in \Omega$. Questa è superiormente limitata da $I = \bigcup I_\alpha$ e inoltre l'ideale nullo appartiene ad Ω. Possiamo dunque applicare il lemma di Zorn poiché le ipotesi sono soddisfatte: abbiamo quindi un elemento massimale P. Ci chiediamo se P è primo. Supponiamo $x, y \notin P$, vogliamo dimostrare che $xy \notin P$. $P + (x) \supsetneq P$ e $P + (y) \supsetneq P$. Dato che P è elemento massimale di Ω esistono m, n tali che $a^n \in P + (x)$ e $a^m \in P + (y)$. Adesso $a^{n+m} \in (xy) + P$. Se $xy \in P$ allora $(xy) + P = P \subset \Omega$, ma questo è assurdo perché $a^{m+n} \in (xy) + P$. Pertanto $xy \notin P$ come volevamo dimostrare. Allora P è un ideale primo e $a \notin P$ ($P \subset \Omega$).

⋈

Proposizione 1.1.6 *Sia* A *anello e* I *un ideale di* A*, allora* $\sqrt{I} = \bigcap_{P \supseteq I} P$ *con* P *ideale primo.*

Dimostrazione: Analoga alla precedente.

⋈

Definizione 1.7 *Chiamiamo* ***radicale di Jacobson*** *di* A *l'ideale* $\mathcal{J}(A) = \bigcap_{M \subseteq A} M$ *con* M *ideale massimale.* $\mathcal{J}(A) \supseteq \mathcal{N}(A)$ *poiché un ideale massimale è primo.*

Proposizione 1.1.7 *Sia A anello. $x \in \mathcal{J}(A) \iff \forall y \in A, (1-xy) \in A^*$.*

Dimostrazione: $\Leftarrow$) Se $x \notin \mathcal{J}(A) \Rightarrow \exists M$ massimale tale che $x \notin M$. Considero l'ideale $(M,x) \supsetneq M$, quindi $(M,x) = A$. Allora esiste $m \in M, y \in A$ tale che $1 = m + xy$ cioè $1 - xy = m \in M$ e questo implica che $(1-xy) \notin A^*$.
$\Rightarrow$) Se $(1-xy) \notin A^*$ allora $\exists M$ massimale tale che $(1-xy) \in M$. Se $xy \in M$ allora $m - xy = 1 \in M$, ma allora M sarebbe tutto l'anello, assurdo. Dunque $xy \notin M$ e quindi $x \notin M, y \notin M$ che è la tesi.

$\bowtie$

Definizione 1.8 *Sia A anello. Se esiste unico ideale massimale M, l'anello si dice* ***locale*** *e si indica con (A, M). Inoltre, se un anello possiede un numero finito di ideali massimali si dice* ***semilocale****.*

ESEMPIO: gli anelli della forma $\mathbb{Z}_{p^a}$ con p primo e $a > 1$ sono anelli locali.
OSSERVAZIONE: Gli ideali di $\mathbb{Z}$ soddisfano le proprietà:

- $(a) + (b) = (a,b) = (d)$, $d = MCD(a,b)$
- $(a) \cap (b) = (m)$, $m = mcm(a,b)$

Definizione 1.9 *Sia A anello e I, J ideali di A. Se $I + J = A$, allora I e J si dicono* ***comassimali***

Proposizione 1.1.8 *Sia A anello e I, J comassimali, allora $I \cap J = IJ$*

Dimostrazione: $I + J = A \Rightarrow \exists i \in I, \exists j \in J$ tali che $i + j = 1$. Sia $\alpha \in I \cap J \Rightarrow \alpha = \alpha(i+j) = \alpha i + \alpha j \in IJ$. Quindi $I \cap J \subset IJ$. L'altra inclusione è banale.

$\bowtie$

La condizione enunciata è sufficiente ma non necessaria, infatti in $\mathbb{K}[x,y]$, $(x) + (y) \neq (1)$, ma $(x) \cap (y) = (xy)$.

Proposizione 1.1.9 *Sia A anello e P ideale primo, se $P \supseteq \bigcap_{i=1}^n I_i$ con I_i ideale $\forall i$, allora $\exists i$ tale che $P \supseteq I_i$. Inoltre, se $P = \bigcap_{i=1}^n I_i$ allora $\exists j$ tale che $P = I_j$.*

Dimostrazione: Supponiamo che $\forall i, P \not\supseteq I_i$, vogliamo dimostrare che $P \not\supseteq \bigcap_{i=1}^n I_i$. $\forall i, \exists x_i \in I_i$ t.c. $x_i \notin P$. Sia $x = x_1 x_2 \cdots x_n$. Adesso $x \notin P$ perché P è primo, mentre $x \in \prod_i I_i \subset \bigcap_{i=1}^n I_i$ e dunque ho la tesi. Se $P = \bigcap_{i=1}^n I_i$ allora $P \subseteq I_i, \forall i$. Per quanto appena detto $\exists j$ t.c. $I_j \subseteq P = \bigcap_{i=1}^n I_i \subseteq I_j$ e questo implica che $P = I_j$.

$\bowtie$

Proposizione 1.1.10 (Lemma di scansamento) *Sia A anello, $P_1, ..., P_n$ ideali primi e sia $I \subseteq A$ ideale tale che $I \subseteq \bigcup_i P_i$. Allora $\exists i$ tale che $I \subseteq P_i$*

Dimostrazione: Dimostriamo la contronominale: $I \nsubseteq P_i, \forall i \Rightarrow I \nsubseteq \bigcup_i P_i$. Procediamo per induzione: il passo base $n = 1$ è banalmente verificato. Supponiamo che la tesi sia vera per $n-1$: allora, sfruttando l'ipotesi induttiva $\forall i, \exists x_i \in I$ tale che $x_i \notin \bigcup_{j \neq i} P_j$. Vorrei far vedere che esiste un elemento α che appartiene a I, ma non appartiene all'unione dei P_i per $i = 1, 2, ..., n$. Se $\exists i$ tale che $x_i \notin P_i$ ho la tesi. Se invece $\forall i, x_i \in P_i$, definisco

$$\alpha = \sum_i \Big(\prod_{j \neq i} x_j \Big)$$

$\alpha \in I$ in quanto somma di elementi di I, ma si verifica che $\forall i, \alpha \notin P_i$ (l'*i-esimo* addendo della somma non appartiene a P_i poiché gli ideali sono primi) e quindi $\alpha \notin \bigcup_i P_i$.

$\bowtie$

Definizione 1.10 *Siano A, B anelli, $f : A \to B$ è detto* ***morfismo di anelli*** *se*

- $f(a+b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$
- $f(1_A) = 1_B$

Notiamo che l'unico omomorfismo di anelli da $\mathbb{Z}$ in $\mathbb{Z}$ è l'identità. Il nucleo e l'immagine di un omomorfismo sono definiti sempre allo stesso modo. Inoltre il *Ker* di un omomorfismo di anelli è un ideale di A e l'immagine è un sottoanello di B. Introduciamo la seguente relazione di equivalenza: sia $I \subseteq A$ ideale, $a \equiv b\ (I) \iff a - b \in I$. Indichiamo la classe di equivalenza (elemento di A/I) con $\bar{a}, [a], a + I$.

Proposizione 1.1.11 *Sia A anello e I ideale. A/I è un anello con le operazioni indotte da A.*

Dimostrazione: Semplici verifiche.

⋈

Definizione 1.11 *Definiamo $\pi : A \to A/I$* ***omomorfismo di proiezione****.*

Se $I \subseteq J \subseteq A$, allora $\pi(J) = J/I$. Si può verificare inoltre che se J è un ideale lo è anche J/I. Esiste inoltre una corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A che contengono I.

Teorema 1.1.12 (Primo teorema di omomorfismo) *Sia $f : A \to B$ omomorfismo di anelli, allora $A/Kerf \cong Imf$.*

Teorema 1.1.13 (Secondo teorema di omomorfismo) *Sia A anello, I,J ideali tali che $I \subseteq J \subseteq A$, allora $(A/I)/(J/I) \cong A/J$.*

Definizione 1.12 *Sia $f : A \to B$ omomorfismo di anelli e siano $I \subseteq A$ e $J \subseteq B$ ideali. Definiamo $J^c = f^{-1}(J) = \{a \in A | f(a) \in J\}$* ***contrazione di J*** *tramite f. Definiamo inoltre $I^e = (f(I)) = \{\sum_i b_i f(a_i) | a_i \in I, b_i \in B\}$* ***ideale esteso di I****.*

Osserviamo che la definizione di ideale esteso è necessaria poiché, in generale, $f(I)$ non è un ideale. Inoltre valgono le seguenti facili proprietà:

- $I \subseteq (I^e)^c$
- $(J^c)^e \subseteq J$
- $(I^e)^{ce} = I^e$
- $(J^c)^{ec} = J^c$

Proposizione 1.1.14 *Sia $f : A \to B$ morfismo di anello, $I \subseteq A, J \subseteq B$ ideali, allora J^c è ideale di A. Inoltre se f è suriettivo, $f(I)$ è un ideale.*

Dimostrazione: Siano $a_1, a_2 \in J^c \Rightarrow f(a_1), f(a_2) \in J \Rightarrow f(a_1 + a_2) = f(a_1) + f(a_2) \in J \Rightarrow a_1 + a_2 \in J^c$. Analogamente il prodotto.
$f(I) \subseteq I^e$, vogliamo mostrare l'inclusione opposta. Sia $\alpha \in I^e \Rightarrow \alpha = \sum_i b_i f(a_i)$ con $a_i \in I$. Dunque per la suriettività di f, $\exists \beta_i \in A$ t.c. $f(\beta_i) = b_i$. Allora $\alpha = \sum_i f(\beta_i) f(a_i) = f(\sum_i \beta_i a_i) \in f(I)$.

⋈

Proposizione 1.1.15 *Sia J ideale primo, allora J^c è primo.*

Dimostrazione: Sia $f : A \to B$ morfismo di anelli, $J \subseteq B$. Se $ab \in J^c$ allora $f(ab) = f(a)f(b) \in J \Leftrightarrow f(a) \in J$ o $f(b) \in J \Leftrightarrow a \in J^c$ o $b \in J^c$.

⋈

Osserviamo invece che J ideale primo non implica J^e ideale primo, per un certo morfismo di anelli (controesempio: con $f : \mathbb{Z} \to \mathbb{Q}$ si consideri l'ideale $2\mathbb{Z}$).

Teorema 1.1.16 *Sia A un anello, I ideale, allora valgono le seguenti proposizioni:*

- *I primo $\iff$ A/I è dominio;*
- *I massimale $\iff$ A/I è campo;*
- *$I = \sqrt{I} \iff$ A/I è ridotto ($\mathcal{N}(A/I) = 0$)*
- *I primario $\iff \mathcal{D}(A/I) = \mathcal{N}(A/I)$*

Dimostrazione:

- $\Rightarrow$) $(a + I)(b + I) = ab + I = I \Leftrightarrow ab \in I$, allora, essendo I primo, $a \in I$ o $b \in I$.
  $\Leftarrow$) $ab \in I \Rightarrow (ab + I) = (a + I)(b + I) = I$, allora, essendo A/I un dominio, $a \in I$ o $b \in I$

- $\Rightarrow$) $\forall m \in A - I, (I, m) = A$ per la massimalità di I. Allora $\exists i \in I, a \in A$ t.c. $i + ma = 1$. $\pi(i + ma) = I + ma = (I + m)(I + a) = 1 + I = \pi(1) \Rightarrow (m + I)$ ammette inverso. Dunque A/I è un campo.
  $\Leftarrow$) Consideriamo un ideale J tale che $I \subseteq J \subseteq A$. Allora $J/I = \pi(J)$ è un ideale poiché π è suriettiva e può essere solamente A/I o (0) poiché il quoziente è un campo. Di conseguenza $J = A$ o $J = I$ rispettivamente; questo implica che I è massimale.

- $\Rightarrow$) Assumere $I = \sqrt{I}$ è equivalente a $a^n \in I \Leftrightarrow a \in I$. Se esistesse un nilpotente $b \in A/I$ t.c. $I = (b + I)^n = b^n + I$ allora $b^n \in I$ e quindi $b \in I$.
  $\Leftarrow$) $a^n \in I \Leftrightarrow a^n + I = I \Leftrightarrow (a + I)^n = I \Leftrightarrow a \in I$ dove l'ultimo "se e solo se" deriva dall'ipotesi che il quoziente è ridotto.

- $\Rightarrow$) Sia $(x + I) \in \mathcal{D}(A/I) \Rightarrow \exists (y + I) \neq I$ tale che $(x + I)(y + I) = xy + I = I \Rightarrow xy \in I$. Dato che $y \notin I$, allora $x^n \in I$ per la primarietà di $I \Rightarrow (x + I) \in \mathcal{N}(A/I)$. Il contenimento opposto è banale.
  $\Leftarrow$) Sia $xy \in I$ e supponiamo che x non appartenga a I. Vorremmo mostrare che $y^n \in I$. $(x + I)(y + I) = xy + I = I$ e dunque $(y + I) \in \mathcal{D}(A/I) = \mathcal{N}(A/I) \Rightarrow y^n \in I$.

⋈

Proposizione 1.1.17 *Sia A anello, $I \subseteq A$ ideale tale che $\sqrt{I} = M$ massimale, allora I è primario.*

Come appena visto, I è primario $\Leftrightarrow \mathcal{N}(A/I) = \mathcal{D}(A/I)$. Osserviamo che se I è ideale primo vale che $P \supseteq I \Rightarrow P \supseteq \sqrt{I}$ (segue dal fatto che un ideale primo è radicale e il passaggio al radicale mantiene le inclusioni). L'ideale M è massimale e quindi primo $M = \sqrt{I} = \bigcap_{P \supseteq I \text{ primo}} P \subseteq M$ e quindi M è l'unico ideale primo che contiene I. Allora l'unico ideale primo di A/I è $M/I \Rightarrow (A/I, M/I)$ è un anello locale e quindi tutti gli elementi non invertibili sono contenuti nell'ideale massimale (sia a non invertibile, allora sappiamo che esiste un ideale massimale che lo contiene) $\Rightarrow M/I = \sqrt{I}/I = \mathcal{N}(A/I) \subseteq \mathcal{D}(A/I) \subseteq \mathcal{J}(A/I) = M/I$.

⋈

Proposizione 1.1.18 *Sia A anello, allora* $\mathcal{D}(A) \cap A^* = \emptyset$. *Inoltre, se A è finito,* $A = \mathcal{D}(A) \cup A^*$.

Dimostrazione: Sia $a \in \mathcal{D}(A) \cap A^*$, allora $\exists b \neq 0, c \in A$ tali che $ab = 0$ e $ac = 1$, ma allora $cab = b = 0$ assurdo.
Se A è finito, prendiamo un $a \notin \mathcal{D}(A)$, vogliamo mostrare che $a \in A^*$. Considero l'applicazione $\varphi : A \to A$ tale che $\varphi(x) = ax$. L'applicazione è iniettiva infatti se $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0$. Essendo φ iniettiva tra insiemi uguali, è anche suriettiva e pertanto esisterà un $w \in A$ tale che $aw = 1 \Rightarrow a \in A^*$.

⋈

Proposizione 1.1.19 *Sia A anello, I ideale tale che* $\forall x \notin I \Rightarrow x \in A^*$, *allora A è locale e I è il suo ideale massimale.*

Dimostrazione: $\forall J \subseteq A \Rightarrow I \supseteq J$ in quanto, se per assurdo $J \nsubseteq I$, esisterebbe $x \in J, x \notin I \Rightarrow x \in A^* \Rightarrow J = A$.

⋈

Proposizione 1.1.20 *Sia A anello, M ideale massimale. Se ogni elemento dell'insieme* $1 + M = \{1 + m | m \in M\}$ *è invertibile, allora A è locale e M è il suo unico ideale massimale.*

Dimostrazione: Voglio provare che se $x \notin M$ allora $x \in A^*$ e poi applicare la proposizione precedente. Per la massimalità di M, $(M, x) = A$, quindi $\exists m \in M, y \in A$ tali che $m + xy = 1 \Rightarrow xy = 1 - m$ è invertibile. Quindi $x \in A^*$ poiché $\exists u \in A$ tale che $(xy)u = x(yu) = 1$.

⋈

Ci chiediamo quale relazione ci sia tra gli ideali di un anello A e quelli di $A[x]$. Abbiamo l'immersione $i : A \to A[x]$. Siano $I \in A, J \in A[x]$ ideali, allora $J^c = i^{-1}(J) = \{a \in A | i(a) = a \in J\} = J \cap A$ e $I^e = (i(I)) = \{\sum_i g_i(x) a_i | a_i \in I, g_i \in A[x]\} = ... = \{\sum_i c_i x^i | c_i \in I\} = I[x]$.

Proposizione 1.1.21 *Sia A anello, I ideale, allora* $A[x]/I[x] \cong (A/I)[x]$.

Dimostrazione: Consideriamo l'omomorfismo di lettura modulo I, $\varphi : A[x] \to (A/I)[x]$ tale che $\varphi(\sum_{i=1}^n b_i x^i) = \varphi(g(x)) = \bar{g}(x) = \sum_{i=1}^n \bar{b_i} x^i$. φ è banalmente suriettiva, inoltre $I[x] \subseteq Ker\varphi$. D'altra parte, se $\varphi(g(x)) = \sum_{i=1}^n \bar{b_i} x^i = 0 \Rightarrow \bar{b_i} = 0 \Rightarrow b_i \equiv 0\ (I)\ \forall i \Rightarrow g(x) \in I[x]$ e quindi $I[x] \supseteq Ker\varphi$. Per il primo teorema di omomorfismo si ha la tesi.

⋈

Proposizione 1.1.22 *Sia A anello e I ideale primo di A, allora, data l'inclusione di A in* $A[x]$, $I^e = I[x]$ *è primo in* $A[x]$.

Dimostrazione: I primo $\Rightarrow A/I$ dominio $\Rightarrow (A/I)[x]$ è dominio, ma allora anche $A[x]/I[x] \cong (A/I)[x]$ è dominio, ovvero $I[x]$ è primo.

⋈

Teorema 1.1.23 *Gli ideali primi di* $\mathbb{Z}[x]$ *sono tutti e soli della forma:*
1)(0)*;*
2)$(f(x))$ *con* $f(x)$ *irriducibile;*
3)$(p)[x]$ *con p primo;*
4)$(p, g(x))$ *con* $g(x)$ *irriducibile modulo p e* (p) *massimale.*

Dimostrazione: Dimostriamo prima che gli ideali indicati sono effettivamente primi e poi che sono tutti e soli. L'ideale 0 è banalmente primo. $(f(x))$ con $f(x)$ irriducibile è primo poiché se $a(x) \in (f(x))$, allora per la fattorizzazione unica $\exists! h(x)$ t.c. $a(x) = h(x)f(x)$ e $f(x) \in (f(x))$. $(p)[x]$ con p primo è un ideale primo per la proposizione precedente. Per dimostrare che $(p, g(x))$ (con $g(x)$ irriducibile modulo p e (p) massimale) è un ideale primo facciamo vedere che il quoziente $\mathbb{Z}[x]/(p, g(x))$ è un campo: per il secondo teorema di omomorfismo abbiamo:

$$\mathbb{Z}[x]/(p, g(x)) \cong (\mathbb{Z}[x]/(p)[x])/((p, g(x))/(p)[x]) \cong \mathbb{Z}_p[x]/(\bar{g}(x))$$

Dato che $g(x)$ è irriducibile modulo p e $\mathbb{Z}_p[x]$ è euclideo, $(\bar{g}(x))$ è massimale (in quanto irriducibile in anello euclideo implica massimale) e il quoziente è un campo. Allora $(p, g(x))$ è massimale e dunque primo.
Dimostriamo adesso che questi sono gli unici ideali primi di $\mathbb{Z}[x]$. Sia $I \subseteq \mathbb{Z}[x]$ ideale primo. Considero la contrazione di I, che sappiamo essere prima, rispetto all'inclusione naturale di $\mathbb{Z}$ in $\mathbb{Z}[x]$: $I^c = I \cap \mathbb{Z}$, abbiamo due casi: $I^c = (p)$ con p primo o $I^c = 0$. Nel primo caso sappiamo che $(p)[x] = I^{ce} \subseteq I$ quindi

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/(p)[x])/(I/(p)[x]) \cong (\mathbb{Z}_p[x]/(I/(p)[x]))$$

Ora $I/(p)[x] \subseteq \mathbb{Z}_p[x]$ o è 0 o è un ideale primo diverso da 0. Rispettivamente I sarà uguale a $(p)[x]$ o a $(p, g(x))$ con $g(x)$ irriducibile modulo p perché in $\mathbb{Z}_p[x]$ un ideale è primo $\Leftrightarrow$ è della forma $(\bar{g}(x))$ con $\bar{g}(x)$ irriducibile. Se invece $I^c = 0$ considero $f \in I$ irriducibile e quindi primitivo (esiste perché I è primo), voglio dimostrare che $I = (f)$, cioè che $\forall g \in I, f|g$. Supponiamo che f non divida $g \Rightarrow f$ non divide nessuno dei fattori irriducibili di g. Poiché $\mathbb{Z}[x]$ non è euclideo non possiamo applicare il lemma di Bezout. Grazie al lemma di Gauss, però, f è irriducibile su $\mathbb{Z}[x] \Leftrightarrow f$ è irriducibile su $\mathbb{Q}[x] \Rightarrow MCD(f, g) = 1$ in $\mathbb{Q}[x]$. Esistono allora $a(x), b(x) \in \mathbb{Q}[x]$ tali che $f(x)a(x) + g(x)b(x) = 1$. Facendo il minimo comune multiplo e raccogliendo i denominatori si ottiene $c(x)f(x) + d(x)g(x) = D$ con $c(x), d(x) \in \mathbb{Z}[x]$ e $D \in \mathbb{Z} - \{0\}$. D è allora combinazione lineare di elementi che appartengono a I, dunque $0 = I \cap \mathbb{Z} \ni D \neq 0$ assurdo.

⋈

Definizione 1.13 *Siano $A_1, ..., A_n$ anelli, definiamo $A_1 \times ... \times A_n$ l'**insieme delle n-uple** $(a_1, ..., a_n)$ con $a_i \in A_i$.*

Notiamo che dotato delle operazioni di somma e prodotto naturali e l'identità $(1_{A_1}, ..., 1_{A_n})$ l'insieme delle n-uple è un anello e gli ideali sono il prodotto degli ideali. In generale non è un dominio.

Teorema 1.1.24 (Teorema del resto cinese per anelli) *Sia A anello, $I_1, ..., I_n$ ideali tali che $(I_i, I_j) = 1 \ \forall i \neq j$. Si consideri*

$$\varphi : A \longrightarrow A/I_1 \times ... \times A/I_n$$

$$a \longrightarrow (\bar{a}_{I_1}, ..., \bar{a}_{I_n})$$

allora:

1. $\prod_{i=1}^n I_i = \bigcap_{i=1}^n I_i$;
2. φ *è suriettiva;*
3. φ *è iniettiva* $\Longleftrightarrow \bigcap_{i=1}^n I_i = 0$.

Dimostrazione:

1. Per induzione sul numero di ideali. Passo base $n = 2$ già dimostrato. Passo induttivo: $n-1 \Rightarrow n$. Vogliamo dimostrare che $(\prod_{i=1}^{n-1} I_i, I_n) = 1$; da ciò segue la tesi poiché $(I_1 \cap ... \cap I_{n-1}) \cap I_n = \prod_{i=1}^{n-1} I_i \cap I_n = \prod_{i=1}^{n} I_i$ dove la prima uguaglianza segue dall'ipotesi induttiva e la seconda dal passo base. Vorremmo trovare $\alpha \in \prod_{i=1}^{n-1} I_i$ e $\beta \in I_n$ tali che $\alpha + \beta = 1$. Sappiamo per ipotesi che $(I_i, I_n) = 1 \ \forall i \neq n \Rightarrow \exists \alpha_i \in I_i, \beta_i \in I_n$ tali che $\alpha_i + \beta_i = 1$. Consideriamo
$$\prod_{i=1}^{n-1} I_i \ni \alpha = \prod_{i=1}^{n-1} \alpha_i = \prod_{i=1}^{n-1} (1 - \beta_i) \Rightarrow \alpha \equiv 1 (I_n)$$
Quindi $\exists \beta \in I_n$ tale che $\alpha + \beta = 1$.

2. Forniamo una soluzione Lagrangiana: considero $x = (a_1, ..., a_n) \in \prod_{i=1}^{n} A/I_i$, voglio mostrare che esiste un $a \in A$ tale che $\varphi(a) = x$. Per ipotesi $\exists \alpha_i^{(j)} \in I_i, \alpha_j^{(i)} \in I_j$ tali che $\alpha_i^{(j)} + \alpha_j^{(i)} = 1$; definiamo $L_i = \prod_{j \neq i} \alpha_j^{(i)}$, allora
$$a = a_1 L_1 + a_2 L_2 + ... + a_n L_n$$
è l'elemento tale che $\varphi(a) = x$. Infatti
$$L_i = \prod_{j \neq i} \alpha_j^{(i)} \equiv \ 0 \ (I_j) \ \forall j \neq i$$
$$L_i = \prod_{j \neq i} \alpha_j^{(i)} = \prod_{j \neq i} (1 - \alpha_i^{(j)}) \equiv \ 1 \ (I_i)$$
si ottiene dunque $a \equiv a_1 \ (I_1)$, ..., $a \equiv a_n \ (I_n)$.

3. $Ker\varphi$ è l'insieme degli elementi mandati a 0 modulo I_i, ovvero gli $a \in Ker\varphi \Leftrightarrow a \in \bigcap_{i=1}^{n} I_i$.

⋈

1.2 L'anello dei polinomi

Definizione 1.14 *Sia $\mathbb{K}$ campo, si definisce $\mathbb{K}[x_1, ..., x_n]$* ***anello di polinomi in n variabili*** *a coefficienti in un campo $\mathbb{K}$.*

Definizione 1.15 *Chiamiamo $X^\alpha = x_1^{a_1} \cdots x_n^{a_n}$ con $\alpha = (a_1, ..., a_n) \in \mathbb{N}^n$* ***monomio****. Con questa definizione è possibile creare una biezione tra l'insieme dei monomi e $\mathbb{N}^n$ in modo naturale:*
$$\varphi : M \longrightarrow \mathbb{N}^n, \ X^\alpha \to (a_1, ..., a_n)$$
Inoltre $f = \sum_\alpha c_\alpha X^\alpha$ con $c_\alpha \in \mathbb{K}$ tali che $c_\beta \neq 0$ per un numero finito di β viene detto ***polinomio*** *e $c_\alpha x^\alpha$ sono chiamati* ***termini****.*

Definizione 1.16 *$I \subseteq \mathbb{K}[x_1, ..., x_n]$ è un* ***ideale monomiale*** *se $\exists E \subseteq \mathbb{N}^n$, $E \neq \emptyset$ tale che $I = (X^\alpha | \alpha \in E)$.*

Osservazione: se $m = X^\beta$ è un monomio, allora $X^\beta \in I = (X^\alpha | \alpha \in E)$ se esiste $\alpha \in E$ tale che $X^\alpha | X^\beta$ o, equivalentemente, $\beta - \alpha \in \mathbb{N}^n$.

La prossima proposizione è di vitale importanza per lo studio degli ideali monomiali e va sempre tenuta a mente quando si incontra un ideale di questo genere:

Proposizione 1.2.1 *Sia $\sum_\alpha c_\alpha X^\alpha \in \mathbb{K}[x_1, ..., x_n]$ e $I = (X^\alpha | \alpha \in E)$, allora $f \in I \Leftrightarrow \forall \alpha \ c_\alpha X^\alpha \in I$.*

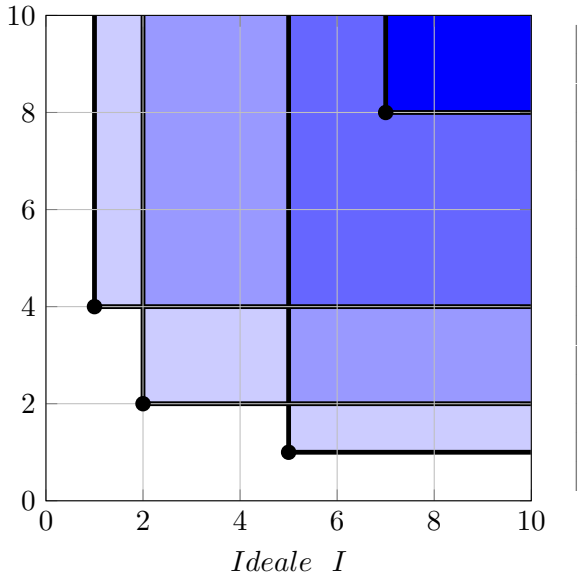
Dimostrazione: $\Leftarrow$) Ovvia;
$\Rightarrow$) $f \in I \Rightarrow \sum_\alpha c_\alpha X^\alpha = f = \sum_{\beta \in E} p_\beta(X) X^\beta = \sum_{\beta \in E}(\sum_\gamma d_{\gamma,\beta} X^\gamma) X^\beta = \sum_{\beta \in E,\gamma} d_{\beta,\gamma} X^{\gamma+\beta}$ con $d_{\beta,\gamma} \in \mathbb{K}$. Voglio far vedere che $\forall \alpha, c_\alpha X^\alpha = d_{\beta,\gamma} X^{\gamma+\beta} \in I$ per certi γ, β. Questo risulta essere vero perché $X^\beta | X^{\gamma+\beta}$ e $X^\beta \in I$ (equivalentemente $(\gamma+\beta) - \beta \in \mathbb{N}^n$).

$\bowtie$

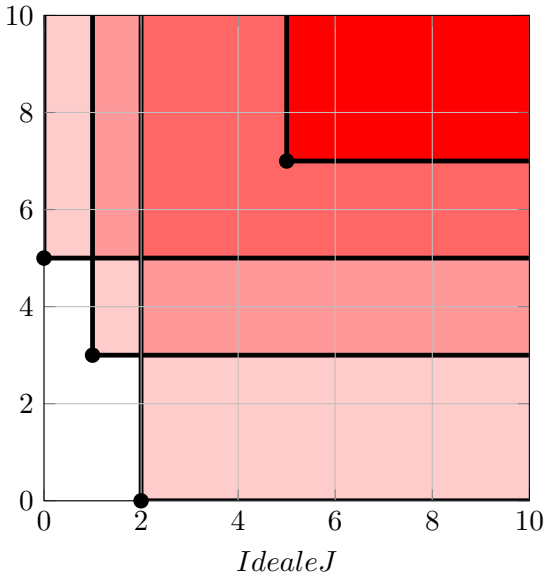
Definizione 1.17 *$E \neq \emptyset \subseteq \mathbb{N}^n$ si chiama **E-sottoinsieme di** $\mathbb{N}^n$ se $\forall \alpha \in E, \forall \beta \in \mathbb{N}^n \Rightarrow \alpha + \beta \in E$.*

Definizione 1.18 *$F \subseteq E$, con E, E-sottoinsieme, si dice **frontiera** se $\forall \alpha \in E, \exists \gamma \in F$ e $\beta \in \mathbb{N}^n$ tali che $\alpha = \gamma + \beta$.*

Cerchiamo di visualizzare la corrispondenza tra un E-sottoinsieme e un ideale in $\mathbb{K}[x, y]$. Consideriamo $I = (xy^4, x^2y^2, x^5y, x^7y^8)$ e $J = (y^5, xy^3, x^2, x^5y^7)$; rappresentiamo le coppie di esponenti come elementi di $\mathbb{N}^2$. Un monomio dell'ideale I (o dell'ideale J) genera tutti i monomi che hanno per esponente una coppia maggiore, componente per componente, alla coppia del monomio assegnato. Questo fatto è rappresentato nei grafici dal piano colorato che genera ogni punto. Un E-sottoinsieme (rappresentato in figura dall'unione dei piani colorati) è quindi l'insieme di tutte le coppie di esponenti $(a, b) \in \mathbb{N}^2$ che può avere un monomio che appartiene ad un ideale.



Ideale I



IdealeJ

Ci possiamo chiedere quando i monomi che non possono essere generati da un ideale monomiale sono in numero limitato. Osservando la figura risulta chiaro che se tra i generatori dell'ideale ci sono tutte le variabili singolarmente, allora i monomi non raggiungibili sono in numero finito.

Notiamo inoltre che gli elementi che appartengono alla frontiera F di un E-sottoinsieme si trovano sul contorno di quest'ultimo. Gli elementi della frontiera sono gli esponenti dei generatori di un ideale monomiale. In particolare, vale il seguente teorema:

Teorema 1.2.2 (Lemma di Dickson) *$\forall E \subseteq \mathbb{N}^n$, E-sottoinsieme esiste una frontiera finita, equivalentemente, ogni ideale monomiale è finitamente generato.*

Dimostrazione: Per induzione su n. Passo base $n = 1$: $E \subseteq \mathbb{N}$ E-sottoinsieme. Essendo $\mathbb{N}$ ben ordinato, la frontiera F è uguale al minimo di E (esiste perché E non è vuoto).
Passo induttivo: $n \Rightarrow n+1$: $E \subseteq \mathbb{N}^{n+1}$ E-sottoinsieme. Considero la proiezione $\pi : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}^n$ tale che $\pi(a_1, ..., a_n, a_{n+1}) = (a_1, ..., a_n)$. Vorremmo dimostrare che $\pi(E) \subseteq \mathbb{N}^n$ è un E-sottoinsieme cosicché, per ipotesi induttiva, sappiamo ammettere frontiera finita. Dati $\alpha \in E, \gamma \in$

$\mathbb{N}^n \Rightarrow \pi(\alpha)+\gamma \in \pi(E)$, infatti $\pi(\alpha+(\gamma,0)) = \pi(\alpha)+\gamma$ in quanto $(\alpha+(\gamma,0)) \in E$. Esiste dunque $\bar{F} = \{\bar{\gamma_1}, ..., \bar{\gamma_k}\}$ frontiera finita di $\pi(E)$. Rimontiamo $\bar{F}$ in $\mathbb{N}^{n+1}$ ottenendo $F_0 = \{\gamma_1, ..., \gamma_k\}$, ma non è detto che ottengo una frontiera poiché l'ultima coordinata dei γ_i potrebbe non essere la minima. Se $\gamma_i = (\gamma_{i,1}, ..., \gamma_{i,n+1})$ considero $\bar{a} = max_i\{\gamma_{i,n+1}\}$ e $E_a = E \cap (\mathbb{N}^n \times \{a\})$ per ogni $a < \bar{a}$ (sono quindi in numero finito), supponendo $E_a \neq \emptyset$. Allora $\pi(E_a)$ avrà una frontiera $\bar{F_a}$ finita (ipotesi induttiva); adesso posso rimontare le frontiere con elementi che hanno in ultima coordinata $a < \bar{a}$ e, considerando $F = F_0 \cup (\cup_a F_a)$, questa è una unione finita. Dobbiamo adesso dimostrare che F è effettivamente frontiera di E. Considero $\alpha = (a_1, ..., a_{n+1}) \in E$:

1. Se $a_{n+1} \geq \bar{a}$, $\exists \beta \in F_0$ tale che $\alpha - \beta \in \mathbb{N}^{n+1}$;
2. Se $a_{n+1} < \bar{a} \Rightarrow \alpha \in E_{a_{n+1}}$, esiste quindi $\gamma \in F_{a_{n+1}}$ tale che $\alpha - \gamma \in \mathbb{N}^{n+1}$.

⋈

Proposizione 1.2.3 *Sia $E \subseteq \mathbb{N}^n$ E-sottoisieme, allora esiste unica frontiera finita di coordinate minimali.*

Dimostrazione: Grazie al lemma di Dickson, sappiamo che esiste una frontiera finita. Sia $N = \{n_1, n_2, ...\} \subseteq \mathbb{N}$ con n_i numero di generatori di una frontiera F_i. N ammette minimo perché sottoinsieme di $\mathbb{N}$. Supponiamo che esistano due indici i, j tale che $n_i = n_j = min(N)$ e che le frontiere associate siano F e G. Dimostriamo che $F = G$. Siano $F = \{a_1, ..., a_k\}$ e $G = \{b_1, ..., b_k\}$ frontiere di coordinate minimali, allora $E = \bigcup_i^k a_i + \mathbb{N}^n = \bigcup_i^k b_i + \mathbb{N}^n$ per definizione di frontiera. Dato che $a_j \in E \Rightarrow a_j \in \bigcup_i^k b_i + \mathbb{N}^n$, in particolare, esiste $\varepsilon(j)$ tale che $a_j \in b_{\varepsilon(j)} + \mathbb{N}^n$. Costruiamo l'applicazione $\varepsilon : \{1, ..., k\} \to \{1, ..., k\}$; notiamo che è surgettiva in quanto, se esistesse z tale che $z \notin Im\varepsilon$, allora $\bigcup_i^k a_i + \mathbb{N}^n \subseteq \bigcup_{i \neq z}^k b_i + \mathbb{N}^n$ e questo è assurdo poiché avrei trovato una frontiera di cardinalità più piccola. La funzione ε è suriettiva tra insiemi finiti di stessa cardinalità e quindi è biettiva. A meno di riordinare i b_i, posso supporre $\varepsilon(i) = i$ e dunque $a_j \in b_j + \mathbb{N}^n$. Sia adesso $b_j \in E$, allora esiste $\eta(j)$ tale che $b_j \in a_{\eta(j)} + \mathbb{N}^n$. Dunque

$$a_j + \mathbb{N}^n \subseteq b_j + \mathbb{N}^n \subseteq a_{\eta(j)} + \mathbb{N}^n$$

Se $j \neq \eta(j)$, allora non è necessario che a_j appartenga alla frontiera; assurdo per ipotesi di minimalità. In conclusione $\forall j, a_j = b_j$.

⋈

Proposizione 1.2.4 (Operazioni tra ideali monomiali) *Dati $I = (m_1, ..., m_k)$, $J = (n_1, ..., n_s)$ ideali monomiali valgono le seguenti proprietà:*

1. *$I + J = (m_1, ..., m_k, n_1, ..., n_s)$;*
2. *$I \cap J = (mcm(m_i, n_j))$ al variare di i, j;*
3. *Se m è un monomio, $I : m = (m_i / MCD(m, m_i))$;*
4. *$I : J = \bigcap_j (I : n_j)$;*
5. *Se m, n sono monomi tali che $MCD(m, n) = 1$, allora $(I, mn) = (I, m) \cap (I, n)$.*

Dimostrazione:

1. Le due inclusioni sono ovvie. Notiamo che l'insieme di generatori, in generale, non è minimale;

2. $\supseteq$) $m_i | mcm(m_i, n_j) \Rightarrow mcm(m_i, n_j) \in I$; analogamente $mcm(m_i, n_j) \in J$;
   $\subseteq$) Sia $\sum_\alpha c_\alpha X^\alpha \in I \cap J$. Per la proposizione 1.2.1 basta far vedere che X^α (cioè i monomi) sono multipli di $mcm(m_i, n_j)$. Dato un monomio $m \in I \cap J$ esistono $u, v \in \mathbb{K}[x_1, ..., x_n]$ e $i, j \in \mathbb{N}$ tali che $m = um_i = vn_j \Rightarrow mcm(m_i, n_j) | m$;

3. $I : m = \{f \in \mathbb{K}[x_1, ..., x_n] | mf \in I\}$. $mf = m \sum_\alpha c_\alpha X^\alpha \in I \Leftrightarrow mX^\alpha \in I$. Inoltre se $MCD(m, m_i) = d_i$, allora $m = a_i d_i$ e $m_i = b_i d_i$ per certi a_i, b_i tali che $MCD(a_i, b_i) = 1$ Dunque $m_i / MCD(m, m_i) = b_i$. La tesi è di conseguenza equivalente a $I : m = (b_1, ..., b_k)$
   $\supseteq$) Devo mostrare che $mb_i \in I$. $mb_i = a_i d_i b_i = a_i m_i \in I$ poiché $m_i \in I$;
   $\subseteq$) Sia u tale che $um \in I$. Grazie alla proposizione 1.2.1 possiamo restringerci al caso in cui u è un monomio; esisteranno allora un certo $v \in \mathbb{K}[x_1, ..., x_n], i \in \mathbb{N}$ tale che $um = vm_i \Rightarrow ua_i d_i = vb_i d_i \Rightarrow b_i | u$ in quanto $MCD(a_i, b_i) = 1$, ovvero $u \in (b_1, ..., b_k)$;

4. $I : J = \{a \in \mathbb{K}[x_1, ..., x_n] | aj \in I, \forall j \in J\}$ e $\bigcap_j (I : n_j) = \bigcap_j (m_i / MCD(m_i, n_j))$ per il punto precedente. Come al solito, grazie alla proposizione 1.2.1, vediamo solamente le inclusioni dei monomi.
   $\supseteq$) $a \in \bigcap_j (m_i / MCD(m_i, n_j)) \Rightarrow \forall j, \exists c_j \in \mathbb{K}[x_1, ..., x_n]$ tale che $a = \dfrac{m_i}{MCD(m_i, n_j)} c_j$. Allora $an_j = \dfrac{m_i n_j}{MCD(m_i, n_j)} c_j$. Notiamo che $\dfrac{n_j}{MCD(m_i, n_j)} \in \mathbb{K}[x_1, ..., x_n]$ e dunque $\forall j, an_j \in I$;
   $\subseteq$) Sappiamo che $a \in (I : J)$ se $\forall j, aj \in I$. In particolare allora $\forall j$, $a \in (I : n_j)$ poiché $n_j \in J$;

5. $\subseteq$) Ovvio;
   $\supseteq$) Sia $v \in (I, m) \cap (I, n)$, $v \notin I$ altrimenti la tesi è banale. Come di consueto, posso supporre v monomio per la proposizione 1.2.1 e pertanto: $v = um = wn$ per certi $u, w \in \mathbb{K}[x_1, ..., x_n]$; visto che $MCD(m, n) = 1$, $m | w \Rightarrow v = kmn \in (I, mn)$ per un qualche $k \in \mathbb{K}[x_1, ..., x_n]$.

⋈

Forniamo un esempio delle varie operazioni: siano $I = (x^2yz^3, xy^2, xz^4)$ e $J = (xy^3, xy^3z, xz^4)$. Notiamo che, in forma minimale, $J = (xy^3, xz^4)$. Allora

- $I + J = (x^2yz^3, xy^2, xz^4, xy^3, xz^4) = (xy^2, xz^4, x^2yz^3)$;
- $I \cap J = (x^2y^3z^3, x^2yz^4, xy^3, xy^2z^4, xy^3z^4, xz^4) = (xy^3, xz^4)$;
- $J = (xz^4, xy^3) = (xz^4, x) \cap (xz^4, y^3) = (x) \cap (x, y^3) \cap (z^4, y^3)$.

Definizione 1.19 *I ideale si dice* ***irriducibile*** *se* $I = I_1 \cap I_2 \Rightarrow I = I_1 \vee I = I_2$

Proposizione 1.2.5 *Sia* $I \subseteq \mathbb{K}[x_1, ..., x_n]$ *monomiale e* $\{m_1, ..., m_k\}$ *insieme di generatori minimale. Allora:*

1. *I massimale* $\Leftrightarrow I = (x_1, ..., x_n)$;
2. *I primo* $\Leftrightarrow I = (x_{i_1}, ..., x_{i_k})$, *ovvero è generato da variabili;*
3. *I radicale* $\Leftrightarrow I = (x_{i_1}x_{i_2} \cdots x_{i_s}, ..., x_{l_1}x_{l_2} \cdots x_{l_t})$, *ovvero è generato da monomi liberi da quadrati;*
4. *I primario* $\Leftrightarrow I = (x_{i_1}^{k_1}, ..., x_{i_s}^{k_s}, m_1, ..., m_t)$ *con* $m_j \in \mathbb{K}[x_{i_1}, ..., x_{i_s}]$;
5. *I irriducibile* $\Leftrightarrow I = (x_{i_1}^{k_1}, ..., x_{i_s}^{k_s})$.

Dimostrazione:

1. $\Rightarrow$) Sia $I = (p_1, ..., p_k)$ con i p_i insieme di generatori monomiali minimale. Se $p_i = x_a x_b$ (eventualmente con $a = b$) allora $(p_1, ..., p_{i-1}, x_a, p_{i+1}, ..., p_k) \supseteq I$ contro la massimalità di I. Inoltre, se $x_j \notin I$ per un certo j, allora $(p_1, ..., p_k, x_j) \supseteq I$ contro la massimalità di I. Pertanto $I = (x_1, ..., x_n)$;
   $\Leftarrow$) A/I è un campo e quindi I è massimale;

2. $\Rightarrow$) Sia $I = (p_1, ..., p_k)$ con i p_i insieme di generatori monomiali minimale. Se $p_i = x_a x_b$ (eventualmente con $a = b$) allora $x_a x_b \in I$, ma $x_a \notin I, x_b \notin I$ contro la primarietà di I. Pertanto $I = (x_{i_1}, ..., x_{i_k})$;
   $\Leftarrow$) A/I è un dominio e quindi I è primo;

3. $\Rightarrow$) Sia $I = (p_1, ..., p_k)$ con i p_i insieme di generatori monomiali minimale. Dire che un ideale è radicale è equivalente a dire che $(a \in I \Leftrightarrow a^n \in I)$. Se $p_i = x_{i_1}^n x_{i_2} \cdots x_{i_s}$ per un certo $n > 1$ (cioè p_i è prodotto di variabili in cui almeno una ha grado strettamente di 1), allora $(x_{i_1} x_{i_2} \cdots x_{i_s})^n \in I$ e di conseguenza $w = x_{i_1} x_{i_2} \cdots x_{i_s} \in \sqrt{I}$, ma $w \notin I$ contro l'ipotesi. Pertanto $I = (x_{i_1} x_{i_2} \cdots x_{i_s}, ..., x_{l_1} x_{l_2} \cdots x_{l_t})$;
   $\Leftarrow$) Mostriamo la tesi equivalente: $(a \in I \Leftrightarrow a^n \in I)$. Per la proposizione 1.2.1 mi basta mostrarla per i monomi. Consideriamo dunque $(X^\alpha)^n \in I$ per un certo $n > 0$,$\alpha = (a_1, ..., a_n)$; voglio mostrare che $X \in I$. Sia quindi $X^\beta \in I$ un monomio, $\beta = (b_1, ..., b_n)$ tale che $n\alpha - \beta \in \mathbb{N}^n$. Per ipotesi β è una stringa composta solamente da 0 e 1 e quindi, se $a_i = 0 \Rightarrow b_i = 0$, se $a_i > 0 \Rightarrow b_i = 0, 1$. Vale quindi che $\alpha - \beta \in \mathbb{N}^n$, cioè la tesi

4. $\Rightarrow$) Sia $I = (p_1, ..., p_k)$ con i p_i insieme di generatori monomiali minimale. $p_i = nx_k$ con $n \notin I$, allora, per la primarietà, $\exists s \in \mathbb{N}$ tale che $x_k^s \in I$. Ma allora p_i può essere solamente o una potenza pura, oppure appartenere a $\mathbb{K}[x_{i_1}, ..., x_{i_t}]$ con le potenze pure di $x_{i_1}, ..., x_{i_t}$ che fanno parte dei generatori;
   $\Leftarrow$) Sia I come nelle ipotesi: a meno di un riordinamento di variabili consideriamo che le potenze pure sono delle variabili $x_1, ..., x_s$. Consideriamo l'immersione $\varphi : \mathbb{K}[x_1, ..., x_n] \to \mathbb{K}(x_{s+1}, ..., x_n)[x_1, ..., x_s]$; allora $\sqrt{\varphi(I)} = (x_1, ..., x_s)$ che è massimale in $\mathbb{K}(x_{s+1}, ..., x_n)[x_1, ..., x_s]$ e quindi $\varphi(I)$ è primario. Consideriamo adesso $\varphi(I)^c$: questo ideale ha gli stessi generatori di I e pertanto $\varphi(I)^c = I$. La contrazione mantiene la primarietà di un ideale e dunque I è primario.

5. $\Rightarrow$) Sia $I = (p_1, ..., p_k)$ con i p_i insieme di generatori monomiali minimale. Supponiamo per assurdo che $p_i = x_a^\alpha x_b^\beta$, allora posso decomporre I come $I = (p_1, ..., p_{i-1}, x_a^\alpha, p_{i+i}, ..., p_k) \cap (p_1, ..., p_{i-1}, x_b^\beta, p_{i+i}, ..., p_k)$ e questa è una decomposizione valida;
   $\Leftarrow$) Supponiamo $I = (x_{i_1}^{k_1}, ..., x_{i_s}^{k_s})$ e che $I = I_1 \cap I_2$. Per come è fatto I, gli elementi che generano gli ideali della sua decomposizione devono essere potenze pure. Chiamiamo allora $(a_1, ..., a_s)$ gli esponenti delle variabili generatrici di I_1 e $(b_1, ..., b_s)$ quelli delle variabili generatrici di I_2. Per ogni coppia (a_i, b_i) uno dei due elementi deve essere uguale a k_i e l'altro più piccolo, altrimenti nell'intersezione ci sarebbe una variabile con esponente minore o maggiore strettamente di k_i, assurdo. Se inoltre esiste j tale che $a_j \neq k_j$ allora considero il prodotto $x_{i_1}^{b_1} x_{i_j}^{a_j}$. Questo elemento appartiene all'intersezione, ma non appartiene invece ad I. Questo implica che $(a_1, ..., a_s) = (k_1, ..., k_s)$ e che quindi $I = I_1$.

$\bowtie$

Abbiamo osservato come è possibile riconoscere un polinomio che appartiene ad un ideale monomiale. Ci chiediamo se è possibile trovare un metodo per capire se un polinomio f appartiene ad un ideale qualsiasi in $\mathbb{K}[x_1, ..., x_n]$. In $\mathbb{K}[x_1]$, essendo un anello euclideo, sappiamo che un elemento $p \in \mathbb{K}[x_1]$ appartiene a un ideale $I = (f_1, ..., f_s) = (MCD(f_1, ..., f_s))$ se è diviso dall'MCD degli $f_1, ..., f_s$. In $\mathbb{K}[x_1, ..., x_n]$, non abbiamo una struttura di anello euclideo e pertanto non

possiamo definire un algoritmo di divisione senza una opportuna funzione grado. Occupiamoci dunque di creare un ordinamento in $\mathbb{K}[x_1, ..., x_n]$.

Definizione 1.20 *Definiamo su $\mathbb{N}^n$, equivalentemente sui monomi di $\mathbb{K}[x_1, ..., x_n]$, " $>$ " **ordinamento monomiale** se:*

1. *" $>$ " è un ordinamento totale (posso confrontare due elementi qualsiasi);*
2. *" $>$ " è un buon ordinamento, ossia ogni sottoinsieme $S \neq \emptyset$ ha minimo, o, equivalentemente, se prendo una successione strettamente decrescente, questa si stabilizza;*
3. *Rispetta la somma, ovvero se $\alpha, \beta \in \mathbb{N}^n, \alpha > \beta$ e $\gamma \in \mathbb{N}^n$ allora $\alpha + \gamma > \beta + \gamma$.*

Diamo tre differenti esempi di ordinamento monomiale (si verifichi per esercizio che sono effettivamente ordinamenti monomiali):

Ordinamento lessicografico: $\alpha, \beta \in \mathbb{N}^n$, allora $\alpha >_L \beta \Leftrightarrow \alpha - \beta$ ha la prima coordinata diversa da 0 da sinistra maggiore di 0;

Ordinamento deg-lex: $\alpha, \beta \in \mathbb{N}^n$, allora $\alpha >_{dL} \beta \Leftrightarrow |\alpha| > |\beta|$ oppure, se $|\alpha| = |\beta|$ allora $\alpha >_L \beta$ con $|\alpha| = \sum_i a_i$ se $\alpha = (a_1, ..., a_n)$;

Ordinamento deg-rev-lex: $\alpha, \beta \in \mathbb{N}^n$, allora $\alpha >_{drL} \beta \Leftrightarrow |\alpha| > |\beta|$ oppure, se $|\alpha| = |\beta|$ allora $\alpha >_{drL} \beta \Leftrightarrow \alpha - \beta$ ha la prima coordinata diversa da 0 da destra negativa.

ESEMPIO: siano $p = x_1^2 x_2 x_3, q = x_1 x_2^3 \in \mathbb{K}[x_1, x_2, x_3]$, allora $p >_L q$, $p >_{dL} q$, $p <_{drL} q$.

Definizione 1.21 *Sia $\sum_\alpha c_\alpha X^\alpha \in \mathbb{K}[x_1, ..., x_n]$, si definisce **multigrado** $Deg(f) = max_>\{\alpha | c_\alpha \neq 0\}$.*

Notiamo che valgono le usuali proprietà della funzione grado, ovvero: $Deg(fg) = Deg(f) + Deg(g)$ e $Deg(f + g) \leq max(Deg(f), Deg(g))$.

Definizione 1.22 *Sia $\sum_\alpha c_\alpha X^\alpha \in \mathbb{K}[x_1, ..., x_n]$ e $\delta = Deg(f)$, si definiscono **leading term**: $lt(f) = c_\delta x^\delta$, **leading monomial**: $lm(f) = x^\delta$, **leading coefficient**: $lc(f) = c_\delta$.*

ESEMPIO: sia $f = 3x^2yz + 5xy^3 + 2x^3$

	Lessicografico	deg-lex	deg-rev-lex
Deg(f)	$(3, 0, 0)$	$(2, 1, 1)$	$(1, 3, 0)$
leading term	$2x^3$	$3x^2yz$	$5xy^3$
leading monomial	x^3	x^2yz	xy^3
leading coefficient	2	3	5

Definizione 1.23 *Siano $f, g, h \in \mathbb{K}[x_1, ..., x_n]$, si dice che **f riduce ad h modulo g**, e si scrive $f \xrightarrow{g} h$, se, detto $\sum_\alpha c_\alpha X^\alpha = \sum_\alpha t_\alpha$, esiste α tale che $lt(g) | t_\alpha$ e $h = f - \frac{t_\alpha}{lt(g)} g$.*

ESEMPIO: siano $f = 6x^2y + 4y^3 - x - 1, g = 2xy + y^2$ con l'ordinamento lessicografico. $lt(g) = 2xy$, allora $h_1 = f - \frac{6x^2y}{2xy} g = -3xy^3 + 4y^3 - x - 1$. Possiamo ancora ridurre: $h_2 = h_1 - (-\frac{3y^2}{2})g = -x - 1 + \frac{3}{2}y^5 + 4y^3$. In conclusione $f \xrightarrow{g} h_2$

Definizione 1.24 *Siano $f \in \mathbb{K}[x_1, ..., x_n]$ e $F = \{f_1, ..., f_s\}$, si dice che **f riduce ad h modulo un insieme F**, e si scrive $f \xrightarrow{F} h$, se esistono indici $i_1, ..., i_t \in \{1, ..., s\}$ e polinomi $h_1, ..., h_{t-1}$ tali che*

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} ... \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

*Si dice che h è **ridotto rispetto a F** se non riesco a fare ulteriori riduzioni, ovvero se $h = 0$ o se $lt(f_i) \nmid d_\beta x^\beta, \forall t_\beta$ termine di h.*

ESEMPIO: $f = x^2y$, $f_1 = xy - x$, $f_2 = x^2 - y$, $F = \{f_1, f_2\}$. Allora

$$f \xrightarrow{f_1} f - xf_1 = x^2 \xrightarrow{f_2} y \qquad quindi \qquad f \xrightarrow{F}_* y, \ ridotto$$

Siamo pronti per definire il seguente:
Algoritmo di divisione:

```
Input: f, f_1, ..., f_s, ">";
    Per ogni i, u_i:=0;
    r:=0;
    h:=f;
    Finché h è diverso da 0, ripeti:
        se esiste i tale che lt(f_i)|lt(h)
            scegli il minimo j con questa proprietà in F={f_1,...,f_s};
            u_j:=u_j+lt(h)/lt(f_j);
            h:=h-f_j*lt(h)/lt(f_j);
        altrimenti
            r:=r+lt(h);
            h:=h-lt(h);
        Fine if
     Fine del ciclo
Output: u_1,...,u_s,r.
```

Proposizione 1.2.6 *L'algoritmo di divisione ha termine in un numero finito di passi e l'output verifica le seguenti condizioni:*

1. $f = \sum_i u_i f_i + r$;
2. r *ridotto rispetto a* $F = \{f_1, ..., f_s\}$;
3. $Deg(f) \geq max(Deg(r), max_i(Deg(u_i fi)))$.

Dimostrazione: L'algoritmo termine grazie al buon ordinamento di " $>$ "; infatti, ad ogni ciclo, il multigrado di h è strettamente minore del suo multigrado al ciclo precedente. La condizione 1 è inoltre soddisfatta per costruzione, infatti ad ogni passo viene aggiunto al termine u_j il monomio che moltiplicato per l'f_i corrispondente viene sottratto ad h (se possibile), altrimenti si aggiunge ad r il monomio che non soddisfa la condizione dell'if. In questo modo si ottiene la decomposizione $f = \sum_i u_i f_i + r$. Analogamente la condizione 2 è soddisfatta poiché a r vengono sommati solamente monomi che non sono divisibili per nessun degli f_i e dunque r è ridotto rispetto a F. La condizione 3 discende dal fatto che r è somma di monomi di $h = f$ e quindi ha multigrado minore o uguale a quello di f, mentre il multigrado dei termini $u_i f_i$ è determinato dal primo ciclo in cui viene scelto l'i corrispondente e può essere solo minore o uguale a quello di f (è possibile ottenere l'uguaglianza solo al primo ciclo dato che poi il multigrado di h cala).

⋈

ESEMPIO: $f = x^2y$, $f_1 = x^2 - y$, $f_2 = xy - x$, $F = \{f_1, f_2\}$, $h = f$, $u_1 = u_2 = r = 0$. $lt(f_1)|lt(h)$ e $lt(f_2)|lt(h)$. Scelgo $i = 1$, $u_1 = 0 + \frac{x^2y}{x^2} = y$, $h := h - yx^2 + y^2 = y^2$. Al secondo passo, nessuno dei $lt(f_i)|lt(h)$ e pertanto $r = y^2$ e $f = yf_1 + y^2$. Notiamo quindi che la divisione dipende dall'ordine con cui si ordinano gli elementi dell'insieme F.

Definizione 1.25 *Sia I ideale e " $>$ " un ordinamento monomiale, si definisce $Lt(I) = (lt(f)|f \in I)$. $Lt(I)$ è monomiale e dunque esiste un insieme finito di generatori, possiamo quindi scegliere $G = \{g_1, ...g_k\} \subseteq I$ tali che $(lt(g_1), ..., lt(g_k)) = Lt(I)$ (equivalentemente $\bigcup Deg(g_i) + \mathbb{N}^n = \bigcup Deg(f) + \mathbb{N}^n$). G prende il nome di* ***base di Gröbner****.*

OSSERVAZIONE: Non tutte le basi sono di Gröbner. Prendiamo $f_1 = x^2+y$, $f_2 = x^2y+1$ e $I = (f_1, f_2) \in \mathbb{K}[x, y]$. L'insieme $\{f_1, f_2\}$ non è una base di Gröbner, infatti in $J = (lt(f_1), lt(f_2)) = (x^2, x^2y) = (x^2)$ non sono contenuti tutti gli elementi di $Lt(I)$ (per esempio il monomio $lt(f_1y - f_2) = lt(x^2y + y^2 - x^2y - 1) = y^2$ non appartiene a J).

Teorema 1.2.7 *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale, e $G = \{g_1, ..., g_t\} \subseteq I$ sono allora fatti equivalenti:*

1. *G è una base Gröbner per I ($Lt(I) = Lt(G)$);*
2. *$f \in I \iff f \xrightarrow{G}_* 0$;*
3. *$f \in I \iff f = \sum_i u_i g_i$ con $Deg(f) \geq Deg(u_i f_i) \forall i$.*

Dimostrazione: Le caratterizzazioni 2 e 3 sono banalmente equivalenti. Dimostriamo quindi le altre due implicazioni:

$1 \Rightarrow 2)$ $\Leftarrow$) Se $r = 0$ allora $f = \sum_i u_i g_i \Rightarrow f \in I$;
$\Rightarrow$) Supponiamo per assurdo $r \neq 0$ con $r = \sum_\alpha r_\alpha X^\alpha$ ridotto ($\forall \alpha | r_\alpha \neq 0, X^\alpha \notin (lt(g_1), ..., lt(g_k))$. $r = f - \sum_i u_i g_i$ e pertanto $r \in I$, ma allora $lt(r) \in Lt(I) = Lt(G)$ e questo è assurdo perché nessuno degli $r_\alpha X^\alpha \in Lt(G)$. Dunque $r = 0$;

$3 \Rightarrow 1)$ Abbiamo banalmente l'inclusione $Lt(G) \subseteq Lt(I)$. Vorremmo mostrare anche l'altra. Sia dunque $f \in I$, allora $f = \sum_{i=1}^t u_i g_i$ con $Deg(f) \geq Deg(u_i g_i)$ $\forall i$. Allora $lt(f) = \sum_i lt(u_i g_i)$ (la somma va intesa solo per i fattori $u_i g_i$ che hanno multigrado uguale a quello di f). L'uguaglianza ci dice che esistono necessariamente polinomi $u_i g_i$ con multigrado uguale a quello di f e che inoltre non può esserci cancellazione numerica totale. Pertanto $\exists j$ tale che $lt(g_j) | \sum_i lt(u_i g_i) = lt(f)$ che è la tesi.

$\bowtie$

Corollario 1.2.8 (Teorema della base di Hilbert) *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale. Allora I è finitamente generato.*

Dimostrazione: Si consideri una base di Gröbner G per I (esiste sempre per come è stata definita). Allora $I = (G) = (g_1, ..., g_k)$ è finitamente generato.

$\bowtie$

Corollario 1.2.9 *Sia $I_1 \subseteq I_2 \subseteq ...$ una catena di ideali in $\mathbb{K}[x_1, ..., x_n]$, allora la successione è stazionaria, cioè $\exists N \in \mathbb{N}$ tale che $\forall k \in \mathbb{N}, I_N = I_{N+k}$.*

Dimostrazione: Consideriamo $I = \bigcup_i I_i$; questo è un ideale che appartiene alla catena. Per il corollario precedente, I è finitamente generato, ovvero $I = (f_1, ..., f_s)$. Esisterà dunque un $N \in \mathbb{N}$ tale che $\{f_1, ..., f_s\} \subseteq I_N$ e pertanto $I \subseteq I_N \subseteq I$ e la catena si stabilizza.

$\bowtie$

Corollario 1.2.10 *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale e $G = \{g_1, ..., g_k\}$ una sua base di Gröbner, allora $\forall f \in \mathbb{K}[x_1, ..., x_n]$, esiste unico r tale che $f \xrightarrow{G}_* r$.*

Dimostrazione: Supponiamo che $f \xrightarrow{G}_* r_1$ e $f \xrightarrow{G}_* r_2$ con $r_1 \neq r_2$. Allora $f = \sum_i u_i g_i + r_1$ e $f = \sum_i h_i g_i + r_2$. Sottraendo membro a membro si ottiene $r_1 - r_2 = \sum_i k_i g_i \in I = (G)$ (quindi $lt(r_1 - r_2)$ deve essere diviso da $lt(g_i)$ per qualche i) e questo è assurdo perché $r_1 - r_2$ è ridotto rispetto a G e pertanto nessuno dei $lt(g_i)$ divide $lt(r_1 - r_2)$. Dunque $r_1 = r_2$.

$\bowtie$

OSSERVAZIONE: Vale anche il viceversa del corollario precedente, ma la dimostrazione non viene riportata.

Come già osservato, non tutte le basi sono di Gröbner. Questo è dovuto al fatto che i polinomi appartenenti all'ideale, cioè le combinazioni lineari di un insieme di generatori $\{f_1, ..., f_s\}$, possono avere leading term di grado minore di quello dei generatori a causa della cancellazione numerica. Diamo allora la seguente definizione che ci aiuterà a capire quando avviene una cancellazione numerica:

Definizione 1.26 *Siano* $f, g \in \mathbb{K}[x_1, ..., x_n]$ *con* $Deg(f) = (a_1, ..., a_n)$, $Deg(g) = (b_1, ..., b_n)$. *Sia* $\gamma = (c_1, ..., c_n)$ *con* $c_i = max(a_i, b_i)$. *Si definisce*

$$\mathcal{S}(f, g) = \frac{X^\gamma}{lt(f)} f - \frac{X^\gamma}{lt(g)} g$$

$\mathcal{S}$-polinomio di f, g. X^γ *è il minimo comune multiplo tra* $X^{Deg(f)}$ *e* $X^{Deg(g)}$.

ESEMPIO: Siano $f_1 = xy^2 + x$, $f_2 = x^2y + y$. Allora $\mathcal{S}(f_1, f_2) = \frac{x^2y^2}{xy^2} f_1 - \frac{x^2y^2}{x^2y} f_2 = x^2 - y^2$.

Dalla definizione e dall'esempio osserviamo che gli $\mathcal{S}$-polinomi sono creati appositamente per causare la cancellazione numerica tra i termini di grado massimo di f_1 e f_2. In questo modo troviamo dei polinomi che hanno leading term diverso dai generatori di un ideale e si può constatare se una base è di Gröbner o meno. Nell'esempio preso in considerazione $\{f_1, f_2\}$ non è una base di Gröbner per $I = (f_1, f_2)$ poiché $lt(\mathcal{S}(f_1, f_2)) \notin (lt(f_1), lt(f_2))$. Il prossimo enunciato, di cui non viene riportata la dimostrazione, mostra come le cancellazioni numeriche possano essere scritte come combinazioni lineari di $\mathcal{S}$-polinomi.

Teorema 1.2.11 *Sia* $f = \sum_{i=1}^{s} c_i X^{\alpha_i} g_i$ *con* $c_i \in \mathbb{K}$ *e* $\{g_1, ..., g_s\}$ *generatori di un ideale* I. *Definiamo* $\forall c_i \neq 0$ $\delta = \alpha_i + Deg(g_i)$ *con* $Deg(f) < \delta$. *Allora* $\exists c_{j,k} \in \mathbb{K}$ *tali che*

$$f = \sum_{j,k} c_{j,k} X^{\delta - \gamma_{j,k}} \mathcal{S}(g_j, g_k)$$

con $X^{\gamma_{j,k}} = mcm(lm(g_j), lm(g_k))$ *e* $Deg(X^{\delta - \gamma_{j,k}} \mathcal{S}(g_j, g_k)) < \delta$.

Per il lemma precedente si può dare la seguente ulteriore caratterizzazione delle basi di Gröbner:

Teorema 1.2.12 (Criterio di Buchberger) *Sia* $I = (g_1, ..., g_k) = (G)$ *ideale. Allora* G *è base di Gröbner se e solo se* $\forall i \neq j$ $\mathcal{S}(g_i, g_j) \xrightarrow{G}_* 0$.

Inoltre è possibile definire un algoritmo che permette di trovare una base di Gröbner a partire da un insieme finito di generatori di un ideale:

Algoritmo di Buchberger

```
Input: F={f_1,...,f_s}, ">"
    G:=F;
    A:={(f_i,f_j)|i<j};
    Finché A è diverso dal vuoto, ripeti
        scegli (f_i,f_j) in A;
        A:=A-{(f_i,f_j)};
        h:=ridotto di S(f_i,f_j) rispetto a G;
        se h diverso da 0
            A:=A+{(g,h)|g in G};
```

```
            G=G unito {h};
         Fine if
    Fine ciclo
Output: G=(g_1,...,g_t) tali che (g_1,...,g_t)=(f_1,...,f_s)
```

Proposizione 1.2.13 *L'algoritmo di Buchberger ha termine.*

Dimostrazione: Chiamiamo G_i l'insieme G al ciclo i-esimo. Ho pertanto la seguente catena di inclusione fra insiemi: $G = G_0 \subseteq G_1 \subseteq G_2 \subseteq ....$ Considero adesso la catena di ideali $Lt(G_0) \subseteq Lt(G_1) \subseteq Lt(G_2)...$ dove le inclusioni ai passi in cui aggiungo un h ridotto diverso da 0 sono strette; questa per il corollario precedente si stabilizza e pertanto, l'algoritmo ha termine.

$\bowtie$

Esempio dell'algoritmo: $f_1 = xy^2 + x$, $f_2 = x^2y + y$, $F = \{f_1, f_2\}$, $A = \{(f_1, f_2)\}$, $G = F$.
Ciclo 1: Calcolo $\mathcal{S}(f_1, f_2) = xf_1 - yf_2 = x^2 - y^2 = f_3$ che non è riducibile rispetto a G e pertanto $G = \{f_1, f_2, f_3\}$. $A = \{(f_2, f_3), (f_1, f_3)\}$.
Ciclo 2: Calcolo $\mathcal{S}(f_2, f_3) = f_2 - yf_3 = y^3 + y = f_4$ che non è riducibile rispetto a G e pertanto $G = \{f_1, f_2, f_3, f_4\}$. $A = \{(f_1, f_3), (f_1, f_4), (f_2, f_4), (f_3, f_4)\}$.
Ciclo 3: Calcolo $\mathcal{S}(f_1, f_3) = xf_1 - y^2f_3 = x^2 + y^4 \xrightarrow{G}_* 0$ e pertanto G rimane invariata. $A = \{(f_1, f_4), (f_2, f_4), (f_3, f_4)\}$.
Ciclo 4: Calcolo $\mathcal{S}(f_1, f_4) = yf_1 - xf_4 = 0$ e pertanto G rimane invariata. $A = \{(f_2, f_4), (f_3, f_4)\}$.
Ciclo 5: Calcolo $\mathcal{S}(f_2, f_4) = y^2f_2 - x^2f_4 = y^3 - yx^2 \xrightarrow{G}_* 0$ e pertanto G rimane invariata. $A = \{(f_3, f_4)\}$.
Ciclo 6: Calcolo $\mathcal{S}(f_3, f_4) = y^3f_3 - x^2f_4 = -y^5 + x^2y \xrightarrow{G}_* 0$ e pertanto G rimane invariata. $A = \emptyset$ e l'algoritmo ha termine con output $G = \{f_1, f_2, f_3, f_4\} = \{xy^2 + x, x^2y + y, x^2 - y^2, y^3 + y\}$

Criterio utile per l'algoritmo: Sia $G = \{g_1, ..., g_s\}$ insieme di generatori, allora se i termini di testa di g_i, g_j sono disgiunti (non hanno variabili in comune), allora $\mathcal{S}(g_i, g_j) \xrightarrow{G}_* 0$. Supponiamo g_i, g_j monici a meno di moltiplicare per l'inverso dei loro leading coefficient e $g_i = X^\alpha + a, g_j = X^\beta + b$ con $MCD(X^\alpha, X^\beta) = 1$, $a = \sum_\gamma c_\gamma X^\gamma$, $b = \sum_\delta d_\delta X^\delta$, $X^\gamma < X^\alpha$ e $X^\delta < X^\beta$. Ora: $\mathcal{S}(g_i, g_j) = X^{\alpha+\beta} + aX^\beta - X^{\alpha+\beta} - bX^\alpha = aX^\beta - bX^\alpha \xrightarrow{g_i} aX^\beta + ba \xrightarrow{g_j} -ab + ba = 0$.

Definizione 1.27 *Sia $G = \{g_1, ..., g_k\}$ una base di Gröbner per I. Se $\forall i$ $lc(g_i) = 1$ e $lt(g_i) \nmid lt(g_j)$ $\forall i \neq j$ allora G è detta* ***base di Gröbner minimale****. Inoltre se $\forall i$ g_i è ridotto rispetto a $(G - \{g_i\})$, cioè nessun monomio di g_i è divisibile per $lt(g_j)$ $\forall j$ allora G prende il nome di* ***base di Gröbner ridotta****.*

Osservazione: Non è detto che l'algoritmo di Buchberger fornisca una base di Gröbner minimale o ridotta.

Osservazione: Se $G_1 = (g_1, ..., g_s), G_2 = (h_1, ..., h_t)$ sono basi di Gröbner minimali allora vale che $s = t$ e, dopo un opportuno riordinamento, $lt(g_i) = lt(h_i)$ $\forall i$.

Proposizione 1.2.14 *Dato un ideale I, esiste ed è unica la base di Gröbner ridotta.*

Dimostrazione: Per l'osservazione precedente possiamo supporre $G = \{g_1, ..., g_s\}$ e $H = \{h_1, ..., h_s\}$ basi di Gröbner ridotte con lo stesso numero di elementi e $lt(g_i) = lt(h_i), \forall i$. Per la caratterizzazione delle base di Gröbner possiamo scrivere $g_j \xrightarrow{H}_* 0$. Dato che g_j è ridotto rispetto a G (e quindi rispetto ad H), l'unico elemento di H che lo può ridurre è h_j. Se adesso $g_j \neq h_j \Rightarrow g_j - h_j$ non è più riducibile e questo è assurdo perché per ipotesi g_j riduce a 0.

$\bowtie$

Abbiamo visto che, dato un ideale I generato da una base di Gröbner ridotta $G = \{g_1, ..., g_s\}$, un polinomio f viene ridotto rispetto a G ad un resto $r = \sum_\alpha r_\alpha X^\alpha$ con $r_\alpha \in \mathbb{K}$. Grazie a questo fatto possiamo interpretare il quoziente $\mathbb{K}[x_1, ..., x_n]/I$ come uno spazio vettoriale sul campo $\mathbb{K}$ generato dai monomi che non sono divisi da nessun $lt(g_i)$ al variare di i. In generale, un tale spazio vettoriale ha dimensione infinita, ma vale il seguente risultato:

Proposizione 1.2.15 *Sia I ideale in $\mathbb{K}[x_1, ..., x_n]$, " $>$ " un ordinamento e $G = \{g_1, ..., g_s\}$ base di Gröbner, allora sono fatti equivalenti:*

- *La dimensione di $\mathbb{K}[x_1, ..., x_n]/I$ come $\mathbb{K}$ spazio vettoriale è finita;*
- *$\forall i = 1, 2..., n, \exists h_i \in I$ tale che $lm(h_i) = x_i^{s_i}$ per un certo $s_i \in \mathbb{N}$;*
- *$\forall i = 1, 2..., n, \exists g_k \in G$ tale che $lm(g_k) = x_i^{\alpha_i}$ per un certo $\alpha_i \in \mathbb{N}$;*

Dimostrazione:

$1 \Rightarrow 2)$ Sia m la dimensione dello spazio vettoriale. Allora, per ogni x_i esiste una combinazione lineare non nulla di $m+1$ vettori tale che $F = \sum_{j=0}^{m} c_j x_i^j = 0$; ovvero $F \in I$ e $lm(F) = x_i^m$;

$2 \Rightarrow 3)$ $h_i \in I \Rightarrow \exists g_j \in G$ tale che $lm(g_j) | lm(h_i) \Rightarrow lm(g_j) = x_i^{\alpha_i}$ per un certo α_i;

$3 \Rightarrow 1)$ Come già osservato, i generatori di $\mathbb{K}[x_1, ..., x_n]/I$ sono tutti i monomi che non sono divisi da nessun $lt(g_i)$ al variare di i. Avendo nella base di Gröbner polinomi con leading monomial $x_i^{\alpha_i}$ $\forall i$, un polinomio ridotto rispetto a G che non appartiene a I sarà della forma $r = \sum_j c_j X^j$ con $j = (j_1, ..., j_n)$ e $j_i < \alpha_i$. Le n-uple j sono in numero finito e pertanto X^j al variare di j sono una base finita di $\mathbb{K}[x_1, ..., x_n]/I$

⋈

Esempio: Sia $I = (x^2 + y, y^3 + z)$; $G = \{x^2 + y, y^3 + z\}$ è una base di Groebner per il criterio visto nelle dispense. Lo spazio vettoriale $\mathbb{K}[x, y, z]/I$ non ha dimensione finita poiché non compare nella base un polinomio con leading monomial del tipo z^α.

Definizione 1.28 *Chiamiamo **ideale 0-dimensionale** un ideale $I \subseteq \mathbb{K}[x_1, ..., x_n]$ tale che $dim(\mathbb{K}[x_1, ..., x_n]/I)$ è finita.*

1.3 Sistemi di equazioni polinomiali

Durante il corso di algebra lineare sono state studiate condizioni necessarie e sufficienti per la risoluzione dei sistemi lineari. In questa parte del corso vorremmo raggiungere il medesimo risultato per quanto riguarda i sistemi polinomiali. In generale cerchiamo quindi un metodo per la risoluzione dei sistemi della forma:

$$\Sigma = \begin{cases} f_1 = 0 \\ f_2 = 0 \\ \vdots \\ f_k = 0 \end{cases} \qquad f_i \in \mathbb{K}[x_1, ..., x_n]$$

In tutta questa parte supporremo il campo $\mathbb{K}$ algebricamente chiuso e useremo costantemente la corrispondenza tra un sistema e l'ideale generato dalle equazioni del sistema. Abbiamo bisogno del seguente lemma preliminare per poter affrontare la trattazione:

Lemma 1.3.1 (Teorema di eliminazione) *Sia $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideale e fissiamo l'ordinamento "$\leq$" lex con $x_1 > x_2 > \cdots > x_n$. Sia G una base di Groebner di I. $\forall\ l = 0, \ldots, n$ definiamo $I_l = I \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$ e $G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$; allora G_l è base di Groebner di I_l.*

Dimostrazione: Osserviamo innanzitutto che la tesi equivale a $Lt(I_l) = (lt(g) | g \in G_l)$. Mostriamo le due inclusioni:

$\supseteq$) Se $g \in G_l$ allora $g \in G \cap \mathbb{K}[x_{l+1}, \ldots, x_n] \subseteq I \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$;

$\subseteq$) Se $m \in Lt(I_l)$ allora $\exists f \in I_l$ tale che $lt(f) = m$. Vogliamo mostrare che $\exists g \in G_l$ tale che $lt(g) \mid lt(f) = m$. Sfruttiamo la seguente proprietà: se $m, n \in \mathbb{K}[x_1, \ldots, x_n]$ sono monomi tali che $x_i \mid m \Leftrightarrow i \in \{1 \ldots, s\}$ e $x_j \mid n \Leftrightarrow j \in \{s+1, \ldots, n\}$, allora $m > n$. Ne consegue che $f \in I_l \subseteq I \Rightarrow \exists g \in G$ t.c. $lt(g) \mid lt(f)$ da cui, per la proprietà esposta sopra, $lt(g) \in \mathbb{K}[x_{l+1}, \ldots, x_n] \Longrightarrow g \in \mathbb{K}[x_{l+1}, \ldots, x_n]$ (perché gli altri termini di g sono minori del *leading term* e sto usando l'ordinamento lessicografico).

$\bowtie$

Definizione 1.29 *Nelle notazioni precedenti chiameremo* ***l-esimo ideale di eliminazione*** *l'ideale $I_l = I \cap \mathbb{K}[x_{l+1}, ..., x_n]$*

Dato il sistema Σ consideriamo l'ideale a lui associato $I = (f_1, ..., f_k) = (g_1, ..., g_s)$ con $G = \{g_1, ..., g_s\}$ base di Groebner; per la definizione di quest'ultima, risolvere il sistema Σ è come risolvere il sistema

$$\Sigma' = \begin{cases} g_1 = 0 \\ \vdots \\ g_s = 0 \end{cases}$$

Per fare ciò consideriamo gli ideali di eliminazione $I_{n-1}, I_{n-2}, ..., I_2, I_1$ (sappiamo come sono fatti per il lemma dimostrato) e procediamo in questo modo: risolviamo il sistema associato a I_{n-1} (lo sappiamo fare poiché sono polinomi in un'unica variabile) e valutiamo I_{n-2} nelle soluzioni trovate; in questo modo I_{n-2} contiene solo polinomi in una variabile e, di nuovo, è possibile trovarne le soluzioni. Procedendo a ritroso in questo modo e "sollevando" le soluzioni il sistema originario, viene risolto. Notiamo però che ci sono problemi: non è sempre possibile sollevare una soluzione e non abbiamo ancora dato condizioni necessarie e sufficienti sulla risolubilità di un sistema polinomiale. Vediamo allora un esempio dando prima però la seguente:

Definizione 1.30 *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$, definiamo* ***varietà affine di I*** *il sottoinsieme di $\mathbb{K}^n$ $\mathcal{V}(I) = \{\alpha \in \mathbb{K}^n | \forall f \in I, f(\alpha) = 0\}$.*

Esempio: Sia $\Sigma = I = (xz - 1, xy - 1)$ una cui base di Groebner è $G = \{xz - 1, xy - 1, y - z\}$;
$I_2 = I \cap \mathbb{K}[z] = (0) \Rightarrow \mathcal{V}(I_2) = \mathbb{K}$
$I_1 = I \cap \mathbb{K}[y, z] = (y - z) \Rightarrow \mathcal{V}(I_2) = \{(a, a) | a \in \mathbb{K}\}$
$\mathcal{V}(I) = \{1/a, a, a) \in \mathbb{K}^3 | a \neq 0\}$
Come anticipato, non tutte le soluzioni dell'ideale di eliminazione più basso possono essere portate al livello superiore. Vedremo più avanti delle condizioni sufficienti al sollevamento.

Osservazione: Non tutti i sottoinsiemi di $\mathbb{K}^n$ sono varietà: prendiamo per esempio la retta reale privata dello 0.

Definizione 1.31 *Sia I ideale, definiamo $\mathcal{I}(\mathcal{V}(I)) = \{f \in \mathbb{K}[x_1, ..., x_n] | f(\alpha) = 0, \forall \alpha \in \mathcal{V}(I)\}$.*

OSSERVAZIONE: In generale vale solamente che $I \subset \mathcal{I}(\mathcal{V}(I))$: basta prendere ad esempio $I = (x^2) \subseteq \mathbb{K}[x]$, $\mathcal{V}(I) = 0$ e $\mathcal{I}(V(I)) = (x)$. Dimostreremo più avanti che, sotto opportune ipotesi, $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.

Definizione 1.32 *Sia R dominio e $f = \sum_{i=0}^{m} a_i x^i, g = \sum_{j=0}^{n} b_j x^j \in R[x]$. Definiamo la* ***matrice di Sylvester*** *appartenente a $M_{m+n}(R)$*

$$Syl(f,g) = \begin{bmatrix} a_m & a_{m-1} & ... & ... & ... & a_0 & 0 & ... & ... & 0 \\ 0 & a_m & a_{m-1} & ... & ... & a_1 & a_0 & 0 & ... & 0 \\ \vdots & & \ddots & & & & & \ddots & & \\ \vdots & & & \ddots & & & & & \ddots & \\ 0 & ... & ... & 0 & a_m & ... & ... & ... & ... & a_0 \\ b_n & b_{n-1} & ... & ... & ... & b_0 & 0 & ... & ... & 0 \\ 0 & b_n & b_{n-1} & ... & ... & b_1 & b_0 & 0 & ... & 0 \\ \vdots & & \ddots & & & & \ddots & & & \\ \vdots & & & \ddots & & & & \ddots & & \\ 0 & ... & ... & ... & 0 & b_n & b_{n-1} & ... & ... & b_0 \end{bmatrix}$$

Definiamo inoltre ***Risultante di*** *f, g: $Ris(f,g) = det(Syl(f,g))$.*

ESEMPIO: $f = ax^2 + bx + c$, $a \neq 0$, $f' = 2ax + b$. Costruiamo

$$Syl(f,f') = \begin{bmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{bmatrix}$$

$Ris(f,f') = -a(b^2 - 4ac)$. Il fatto che il risultante si annulli esattamente quando lo fa il discriminante di una equazione di secondo grado ci fa intuire la proprietà fondamentale del risultante e cioè che $Ris(f,g) = 0 \Leftrightarrow f, g$ hanno fattori in comune non banali.

Elenchiamo adesso alcune proprietà del risultante: le prime tre discendono direttamente da quelle del determinante, mentre l'ultima viene assunta come definizione.

Proposizione 1.3.2 ***Proprietà del risultante:***

1. *$Ris(f,g) \in R$ (se $R = \mathbb{K}[y]$ e $f, g \in \mathbb{K}[x,y] = \mathbb{K}[y][x] \Rightarrow Ris(f,g) \in \mathbb{K}[y]$);*
2. *$Ris(g,f) = (-1)^{mn} Ris(f,g)$;*
3. *$Ris(af, g) = a^n Ris(f,g)$ con $a \in R$;*
4. *$Ris(a,f) = a^n$, $Ris(a,b) = 1$ con $a, b \in R$*

Siano adesso $z_1, ..., z_m$ indeterminate e consideriamo il polinomio monico $f_m(x) = \prod_{i=1}^{m}(x - z_i) = \sum_{i=0}^{m} a_i^{(m)} x^i$ con $a_i^{(m)}$ funzione simmetrica elementare degli z_i:

$$\begin{cases} a_m^{(m)} = 1 \\ a_{m-1}^{(m)} = -(z_1 + ... + z_m) = (-1)^1 \sum_{i=1}^{m} z_i \\ a_{m-2}^{(m)} = z_1 z_2 + z_1 z_3 + ... + z_{n-1} z_n = (-1)^2 \sum_{i<j} z_i z_j \\ \vdots \\ a_0^{(m)} = (-1)^m z_1 z_2 \cdots z_m \end{cases}$$

Osserviamo che $a_i^{(m)}$ sono lineari in ognuna delle variabile z_i. Definiamo inoltre $f_{m-1}(x) = \frac{f_m(x)}{x-z_m} = \sum_{i=0}^{m-1} a_i^{(m-1)} x^i$ e notiamo che vale la relazione

$$a_{i-1}^{(m-1)}(z_1, ..., z_{m-1}) = a_i^{(m)}(z_1, ..., z_{m-1}, 0)$$

Siamo pronti a dimostrare il seguente

Lemma 1.3.3 *Sia R dominio, $g(x) = \sum_{i=0}^{n} b_i x^i \in R[x]$, allora $Ris(f_m, g) = g(z_m) Ris(f_{m-1}, g)$.*

Dimostrazione: Consideriamo la matrice di Sylvester associata e sommiamo all'ultima colonna la i-esima colonna moltiplicata per z_m^{m+n-i} per ogni i; otteniamo dunque il vettore:

$$\begin{pmatrix} z_m^{n-1} f_m(z_m) \\ z_m^{n-2} f_m(z_m) \\ \vdots \\ f_m(z_m) \\ z_m^{m-1} g(z_m) \\ z_m^{m-2} g(z_m) \\ \vdots \\ g(z_m) \end{pmatrix} = g(z_m) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ z_m^{m-1} \\ z_m^{m-2} \\ \vdots \\ 1 \end{pmatrix}$$

Nella posizione $j = 1, ..., n$ dell'ultima colonna ottengo il valore $z_m^{n-j} f_m(z_m)$ che vale 0 poiché z_m è radice di f_m. Per la multilinearità del determinante posso portare fuori un fattore $g(z_m)$ dall'ultima colonna (chiamo A la matrice così ottenuta), quindi $det(Syl(f_m, g)) = g(z_m) det(A)$, ma $g(z_m)$ ha grado n come polinomio in z_m, d'altra parte gli $a_i^{(m)}$ sono lineari in z_m e dunque il grado di $det(Syl(f_m, g))$ è al massimo n. Di conseguenza $det(A)$ non dipende da z_m per questioni di grado. Posso quindi porre $z_m = 0$ in A e sviluppare il determinante lungo l'ultima colonna di A. Grazie alla relazione tra i coefficienti di f_{m-1} e f_m scritta sopra $det(A) = det(Syl(f_{m-1}, g))$.

⋈

Teorema 1.3.4 *Sia R dominio e $f = a_m \prod_{i=1}^{m}(x - \alpha_i)$, $g = b_n \prod_{j=1}^{n}(x - \beta_j) \in R[x]$ con $\alpha_i, \beta_j \in \overline{R}, \forall i, j$, allora:*

1. $Ris(f, g) = (-1)^{mn} b_n^m \prod_{i=0}^{n} f(\beta_i)$
2. $Ris(f, g) = a_m^n \prod_{i=0}^{m} g(\alpha_i)$
3. $Ris(f, g) = a_m^n b_n^m \prod_i \prod_j (\alpha_i - \beta_j)$

Dimostrazione: Seguono direttamente dal lemma precedente.

⋈

Corollario 1.3.5 (Proprietà fondamentale del risultante:) $Ris(f, g) = 0 \Leftrightarrow \exists h \in R[x]$ *tale che $deg(h) > 0$ fattore comune di f e g.*

Dimostrazione: $0 = Ris(f, g) = a_m^n b_n^m \prod_i \prod_j (\alpha_i - \beta_j) \Leftrightarrow \alpha_i = \beta_j$ per qualche $i, j \Leftrightarrow \exists h \in R[x]$ fattore comune ($deg(h) > 0$) di f, g.

⋈

Teorema 1.3.6 *Siano $f = \sum_{i=0}^{m} a_i x^i, g = \sum_{i=0}^{n} b_i x^i \in R[x]$ con R dominio, allora esistono $A, B \in R[x]$ con $deg(A) < n$, $deg(B) < m$ tali che $Af + Bg = Ris(f, g)$. Pertanto $Ris(f, g) \in (f, g)$*

Dimostrazione: Per calcolare $Ris(f,g)$, moltiplichiamo per ogni i l'i-esima colonna di $Syl(f,g)$ per x^{m+n-i} e la sommiamo all'ultima colonna. Otteniamo pertanto il vettore:

$$\begin{pmatrix} x^{n-1}f(x) \\ x^{n-2}f(x) \\ \vdots \\ f(x) \\ x^{m-1}g(x) \\ \vdots \\ g(x) \end{pmatrix}$$

Svolgendo il determinante lungo questa colonna ed osservando che gli altri elementi della matrice appartengono a R (pertanto il grado dipende solamente dal grado della variabile che moltplica $f(x)$ o $g(x)$), si ottiene la tesi.

⋈

Corollario 1.3.7 *Se $R = \mathbb{K}[y_1, ..., y_t]$ e $f, g \in \mathbb{K}[y_1, ..., y_t, x] = R[x]$ allora $Ris(f,g) \in (f,g) \cap R$, ovvero, $Ris(f,g)$ appartiene al primo ideale di eliminazione di (f,g).*

Dimostrazione: Segue dalle proprietà di determinante e dal teorema precedente.

⋈

Proposizione 1.3.8 *Siano $f, g_1, g_2 \in R[x]$ con R dominio, α_i radici di f, $deg(g_1) = n_1$, $deg(g_2) = n_2$, $n_1 + n_2 = n$, allora $Ris(f, g_1g_2) = Ris(f,g_1)Ris(f,g_2)$ e, se $deg(fg_1 + g_2) = l$, $Ris(f, fg_1 + g_2) = a_m^{l-n_2} Ris(f, g_2)$.*

Dimostrazione: $Ris(f, g_1g_2) = a_m^n \prod_i (g_1g_2)(\alpha_i) = a_m^{n_1} \prod_i g_1(\alpha_i) a_m^{n_2} \prod_i g_2(\alpha_i) = Ris(f,g_1)Ris(f,g_2)$.
Inoltre: $Ris(f, fg_1 + g_2) = a_m^l \prod_i (fg_1 + g_2)(\alpha_i) = a_m^{l-n_2}\big(a_m^{n_2} \prod_i g_2(\alpha_i)\big) = a_m^{l-n_2} Ris(f, g_2)$

⋈

Esercizio: Siano $f, g \in \mathbb{Z}[x]$ con $deg(f) > 0, deg(g) > 0$, monici e $Ris(f,g) = p \in \mathbb{Z}$ primo; sia inoltre $I = (f,g)$. Dimostrare che, se $i : \mathbb{Z} \to \mathbb{Z}[x]$ è l'immersione naturale, allora $I \cap \mathbb{Z} = I^c = (p)$. Calcolare inoltre I^c e $\mathbb{Z}[x]/I$ con $I = (x^2 - 4x + 1, x^2 - x)$.

Soluzione: Notiamo innanzitutto che, per le proprietà del risultante, $p \in I \cap \mathbb{Z}$ e quindi $(p) \subseteq I^c$. Se esistesse un altro elemento $a \in I^c \Rightarrow I^c = \mathbb{Z} \Rightarrow \mathbb{Z} \subseteq I \Rightarrow \exists A, B \in \mathbb{Z}[x]$, $deg(B) < deg(f), deg(A) < deg(g)$ tali che $Af + Bg = 1$. Leggendo questa uguaglianza modulo p abbiamo che $\bar{A}\bar{f} + \bar{B}\bar{g} = \bar{1}$ ($\bar{f}, \bar{g}$ sono coprimi), ma questo è assurdo perché $\overline{Ris(f,g)} = Ris(\bar{f}, \bar{g}) \equiv 0 \pmod p$ ($\bar{f}, \bar{g}$ hanno un fattore comune). L'uguaglianza $\overline{Ris(f,g)} = Ris(\bar{f}, \bar{g})$ deriva dal fatto che f, g sono monici e pertanto la dimensione della matrice di Sylvester associata rimane invariata.
Se $I = (x^2 - 4x + 1, x^2 - x)$, allora $Ris(x^2 - 4x + 1, x^2 - x) = -2$ e pertanto, per dimostrazione precedente, $I^c = (2)$. Possiamo dunque scrivere $I = (I, 2) = (x^2 + 1, x^2 - x, 2) = (x - 1, 2)$ e dunque $\mathbb{Z}[x]/I = \mathbb{Z}_2$.

Osservazione: Con il risultante è possibile costruire polinomi con particolari radici in funzione di quelle di f, g:

Somma delle radici $H_1(x) = Ris_y(f(x - y), g(y)) = (-1)^{mn} a_m^n b_n^m \prod_{i,j} (x - (\alpha_i + \beta_j))$

Differenza delle radici $H_2(x) = Ris_y(f(x + y), g(y)) = (-1)^{mn} a_m^n b_n^m \prod_{i,j} (x - (\alpha_i - \beta_j))$

Prodotto delle radici $H_3(x) = Ris_y(y^m f(x/y), g(y)) = (-1)^{mn} a_m^n b_n^m \prod_{i,j} (x - \alpha_i\beta_j)$

La matrice di Sylvester nasce dall'esigenza di voler trovare un modo per capire se due polinomi avessero o meno dei fattori in comune. In particolare si vuole trovare una condizione che ci dica se due polinomi hanno un fattore comune sapendo che esiste una loro combinazione che fa 0. Sviluppando il sistema $Af + Bg = 0$ nelle variabili "coefficienti di A, B" si ottiene la matrice di Sylvester. Da questa idea è stata sviluppata la teoria del risultante.

Teorema 1.3.9 (Teorema di estensione) *Sia $I \in \mathbb{K}[x_1, ..., x_n]$ ideale, $I = (f_1, ..., f_k)$, $I_1 = \mathbb{K}[x_2, ..., x_n] \cap I$. Possiamo leggere $I \subseteq \mathbb{K}[x_2, ..., x_n][x_1]$ e siano quindi $f_i = g^{(i)}(x_2, ..., x_n)x_1^{n_i} + \bar{f}_i$ con $deg(\bar{f}_i, x_1) < n_i$ per $i = \{1, ..., k\}$. Se $\alpha \in \mathcal{V}(I_1)$ e $\alpha \notin \mathcal{V}((g^{(1)}, ..., g^{(k)}))$ allora $\exists a \in \mathbb{K}$ tale che $(a, \alpha) \in \mathcal{V}(I)$.*

Dimostrazione: La dimostrazione si effettua per il caso $k = 2$. Sia quindi $I = (f, g)$ con $f = a(x_2, ..., x_n)x_1^m + \bar{f}$ e $g = b(x_2, ..., x_n)x_1^s + \bar{g}$ con $deg(\bar{f}, x_1) < m$, $deg(\bar{g}, x_1) < s$. $H(x_2, ..., x_n) = Ris_{x_1}(f, g) \in \mathbb{K}[x_2, ..., x_n] \cap I \Rightarrow Ris_{x_1}(f, g) \in I_1$. Sia $\alpha \in \mathcal{V}(I_1) \Rightarrow H(\alpha) = 0$. Devo fare vedere che fare il risultante e valutarlo in α è come valutare f, g in (x_1, α) e poi farne il risultante, ovvero $H(\alpha) = Ris(f(x_1, \alpha), g(x_1, \alpha))$. Se $a(\alpha) \neq 0$ e $b(\alpha) \neq 0$, allora la matrice di Sylvester associata ha dimensione $(m + s) \times (m + s)$ e questo è sufficiente per far si che risultante e valutazione commutino (poiché le operazioni per il calcolo del determinante coinvolgono solo somme e prodotti). Supponiamo adesso che $a(\alpha) \neq 0, b(\alpha) = 0$, ma allora $Ris(f, x_1^N f + g) = Ris(f, g)$ e la matrice ha la stessa dimensione e possiamo concludere come prima. Se pertanto $\alpha \notin \mathcal{V}(a(x_2, ..., x_n), b(x_2, ..., x_n))$ allora $Ris(f(x_1, \alpha), g(x_1, \alpha)) = 0$ e per la proprietà fondamentale del risultante $\exists a \in \mathbb{K}$ tale che $f(a, \alpha) = g(a, \alpha) = 0$.

⋈

Esempio: Sia $I = (x^3 + 2y + z + t^3, xyz - t, xt + y)$; il coefficiente di x^3 non si annulla mai e pertanto possiamo applicare il teorema di estensione. Notiamo in particolare che se il coefficiente $g^{(1)}(x_2, ..., x_n)$ è una costante, allora vale il teorema di estensione.

Se consideriamo la mappa $\pi : \mathcal{V}(I) \in \mathbb{K}^n \to \mathcal{V}(I_1) \in \mathbb{K}^{n-1}$ tale che $\pi(a_1, ..., a_n) = (a_2, ..., a_n)$, in generale vale $\pi(V(I)) \subseteq \mathcal{V}(I_1)$, se siamo nelle ipotesi del teorema di estensione, vale l'uguaglianza.

Lemma 1.3.10 *Sia $f(x_1, ..., x_n) \in \mathbb{K}[x_1, ..., x_n]$ con $deg(f, x_1) > 0$, allora esiste un cambiamento lineare della forma*

$$\begin{aligned} x_1 &= \bar{x_1} \\ x_2 &= \bar{x_2} + c_2\bar{x_1} \\ &\vdots \\ x_n &= \bar{x_n} + c_n\bar{x_1} \end{aligned}$$

tale che $f(\bar{x_1}, ..., \bar{x_n}) = c_1{\bar{x_1}}^N + \bar{f}$ con $c_1 \neq 0$ e $deg(\bar{f}, \bar{x_1}) < N$

Dimostrazione: Posso scrivere f nella forma $f = f_N + f_{N-1} + ... + f_0$ con $f_i = A_1^{(i)}m_1^{(i)} + ... + A_k^{(i)}m_k^{(i)}$ con $m_j^{(i)} = x_1^{a_1} \cdots x_n^{a_n}$ con $a_1 + ... + a_n = i$ e $A_j^{(i)} \in \mathbb{K}$. Consideriamo adesso, semplificando la notazione, $f_N = A_1m_1 + ... + A_km_k$ con gli m_i come sopra. Applico la trasformazione al primo monomio:

$$m = A_1m_1 = A_1{\bar{x_1}}^{a_1}(\bar{x_2} + c_2\bar{x_1})^{a_2} \cdots (\bar{x_n} + c_n\bar{x_1})^{a_n} = A_1c_2^{a_2} \cdots c_n^{a_n}{\bar{x_1}}^N + g$$

con $deg(g, \bar{x_1}) < N$. Procedendo analogamente per ogni altro monomio di f_N si ottiene $f(\bar{x_1}, ..., \bar{x_n}) = f_N(1, c_2, ..., c_n){\bar{x_1}}^N + \bar{f}$ con $deg(\bar{f}, \bar{x_1}) < N$ e $f_N \in \mathbb{K}[\bar{x_1}, ..., \bar{x_n}]$. Adesso dobbiamo solo mostrare che $c_1 = f_N(1, c_2, ..., c_n)$ è diverso da 0. Notiamo che $f_N(x_1, ..., x_n) \neq 0 \Leftrightarrow f_N(1, x_2, ..., x_n) \neq 0$, ovvero $f_N(1, x_2, ..., x_n)$ non è il polinomio nullo e quindi esistono $c_2, ..., c_n$ tali che $f_N(x_1, c_2, ..., c_n) \neq 0$.

⋈

Teorema 1.3.11 (Hilbert Nullstellensatz (teorema degli zeri di Hilbert)) *Sia $\mathbb{K}$ algebricamente chiuso e $I \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale, allora:*

Forma debole: $\mathcal{V}(I) = \emptyset \iff I = (1)$

Forma forte: $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$

Dimostrazione:

Forma debole: $\Leftarrow$) Banale;
$\Rightarrow$) Per induzione sul numero n di variabili: passo base $n = 1$: $I \subseteq \mathbb{K}[x_1]$, se $I \neq (1) \Rightarrow I = (f(x_1))$ con $\deg(f) > 0 \Rightarrow \exists \alpha \in \mathbb{K}$ tale che $f(\alpha) = 0$ per il teorema fondamentale dell'algebra.
Passo induttivo $(n-1) \Rightarrow n$: Sia $I \in \mathbb{K}[x_1, ..., x_n]$, considero $I_1 \in \mathbb{K}[x_2, ..., x_n]$ per il quale vale l'ipotesi induttiva. Se $I = I_1$ ho finito, altrimenti $\exists f(x) \in I$ tale che $deg(f, x_1) > 0$. Per il lemma, a meno di un cambiamento di coordinate, posso supporre $f = cx_1^N + \bar{f}$ con $deg(\bar{f}, x_1) < N$. Considero ora la proiezione $\pi : \mathbb{K}^n \to \mathbb{K}^{n-1}$ tale che $\mathcal{V}(I) \to \mathcal{V}(I_1)$. Per il teorema di estensione la proiezione è surgettiva e quindi vale l'uguaglianza $\pi(\mathcal{V}(I)) = \mathcal{V}(I_1)$; $\mathcal{V}(I) = \emptyset \Rightarrow \pi(\mathcal{V}(I)) = \mathcal{V}(I_1) = \emptyset \Rightarrow 1 \in I_1$ per ipotesi induttiva $\Rightarrow 1 \in I$.

Forma forte: $\supseteq$) Sia $f \in \sqrt{I} \Rightarrow \exists m \in \mathbb{N}$ tale che $f^m \in I$, allora $\forall \alpha \in \mathcal{V}(I), f^m(\alpha) = (f(\alpha))^m = 0 \Rightarrow f(\alpha) = 0\ \forall \alpha \in \mathcal{V}(I) \Rightarrow f \in \mathcal{I}(\mathcal{V}(I))$;
$\subseteq$) $f \in \mathcal{I}(\mathcal{V}(I))$. Si usa il trucco di Robsnovich: considero l'ideale $J = (I, 1 - tf) \subseteq \mathbb{K}[x_1, ..., x_n, t]$. Voglio mostrare che $\mathcal{V}(J) = \emptyset$ (sto aggiungendo moralmente l'inverso di f modulo I). Se $\alpha = (a_1, ..., a_n, b) \in \mathcal{V}(J) \Rightarrow (a_1, ..., a_n) \in \mathcal{V}(I)$ e α annulla $1 - tf$, ma $1 - tf(\alpha) = 1$ assurdo. Pertanto $\mathcal{V}(J) = \emptyset \Rightarrow 1 \in J$ per la forma debole del teorema, allora $1 = \sum_i h_i(x_1, ..., x_n, t) f_i + (1 - tf) h(x_1, ..., x_n, t)$. Dato che a sinistra abbiamo una costante, l'uguaglianza è vera per ogni valutazione, in particolare posso porre $t = 1/f$ quindi $1 = \sum_i h_i(x_1, ..., x_n, 1/f) f_i + 0$. Facendo il minimo comune multiplo otteniamo: $1 = \frac{1}{f^m} \sum_i \tilde{h_i}(x_1, ..., x_n) f_i \Rightarrow f^m = \sum_i \tilde{h_i}(x_1, ..., x_n) f_i \Rightarrow f^m \in I \Rightarrow f \in \sqrt{I}$

⋈

Proposizione 1.3.12 *Siano I_1, I_2 ideali, $W_1 = \mathcal{V}(I_1)$, $W_2 = \mathcal{V}(I_2)$, valgono le seguenti proprietà:*

1. *Se $I_1 \subseteq I_2 \Rightarrow \mathcal{V}(I_1) \supseteq V(I_2)$;*
2. *Se $W_1 \subseteq W_2 \Rightarrow \mathcal{I}(W_1) \supseteq \mathcal{I}(W_2)$;*
3. *$\mathcal{V}(\mathcal{I}(W_1)) = W_1$;*
4. *Se $\mathbb{K} = \bar{\mathbb{K}}$ e $I_1 = \sqrt{I_1} \Rightarrow \mathcal{I}(W_1) = I_1$ (in generale vale solo $\mathcal{I}(W_1) \supseteq I_1$)*

Dimostrazione: Derivano direttamente dalle definizioni e dal teorema egli zeri.

⋈

Proposizione 1.3.13 *Siano V_1, V_2 varietà affini, allora $\mathcal{I}(V_1) = \mathcal{I}(V_2) \Leftrightarrow V_1 = V_2$*

Dimostrazione: Se $V_1 = V_2$ allora banalmente segue $\mathcal{I}(V_1) = \mathcal{I}(V_2)$. Viceversa supponiamo $\mathcal{I}(V_1) = \mathcal{I}(V_2)$: applicando la varietà ad entrambi i membri si ha che $\mathcal{I}(V_1) = \mathcal{I}(V_2) \Rightarrow \mathcal{V}(\mathcal{I}(V_1)) = \mathcal{V}(\mathcal{I}(V_2)) \Rightarrow V_1 = V_2$ dove l'ultima implicazione deriva dal punto 3 della proposizione precedente. *Dimostrazione alternativa del viceversa (praticamente inutile)*: supponiamo $V_1 = \mathcal{V}(I)$, $V_2 = \mathcal{V}(J)$ e $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathcal{V}(J))$. Mostriamo prima che, dato un ideale I, $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$: visto che $I \subseteq \sqrt{I} \Rightarrow V(\sqrt{I}) \subseteq \mathcal{V}(I)$. Per l'altro contenimento supponiamo $\alpha \in \mathcal{V}(I)$ e sia $g \in \sqrt{I}$ cioè $\exists m \in \mathbb{N}$ tale che

$g^m \in I$, allora $g^m(\alpha) = 0 \Rightarrow g(\alpha) = 0$ poiché $\mathbb{K}[x_1, ..., x_n]$ è un dominio $\Rightarrow \alpha \in \mathcal{V}(\sqrt{I})$. Tornando alla dimostrazione, per il teorema degli zeri si ha che $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathcal{V}(J)) \Rightarrow \sqrt{I} = \sqrt{J}$; dunque $\mathcal{V}(\sqrt{I}) = \mathcal{V}(\sqrt{J})$ e, per quanto dimostrato, $\mathcal{V}(I) = \mathcal{V}(J)$.

⋈

Grazie ai risultati precedenti possiamo caratterizzare gli ideali massimali in un campo algebricamente chiuso.

Proposizione 1.3.14 *Sia $M \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale, allora M è massimale se e solo se $M = (x_1 - a_1, ..., x_n - a_n)$ con $a_i \in \mathbb{K}$. Pertanto vi è una corrispondenza biunivoca tra i punti di $\mathbb{K}^n$ e gli ideali massimali di $\mathbb{K}[x_1, ..., x_n]$.*

Dimostrazione: $\Leftarrow$) Vera in generale: consideriamo la mappa di valutazione: $v : \mathbb{K}[x_1, ..., x_n] \to \mathbb{K}[x_1, ..., x_n]/M \cong \mathbb{K}$ tale che $v(f(x_1, ..., x_n)) = f(a_1, ..., a_n)$. Dato che $\mathbb{K}$ è un campo, si ha la tesi.
$\Rightarrow$) M è massimale $\Rightarrow M \neq (1)$, allora, per il teorema degli zeri, $\mathcal{V}(M) \neq \emptyset \Rightarrow \exists p = (a_1, ..., a_n) \in \mathcal{V}(M)$. Vediamo $p = \mathcal{V}(\mathcal{I}(p)) \subseteq \mathcal{V}(M)$ e dunque, per la proposizione precedente, $\mathcal{I}(p) \supseteq \mathcal{I}(\mathcal{V}(M))$. Notiamo che $\mathcal{I}(p) = (x_1 - a_1, ..., x_n - a_n)$ e, per quanto detto, deve contenere $\mathcal{I}(\mathcal{V}(M)) = \sqrt{M} = M$, ma M è massimale e quindi vale l'uguaglianza.

⋈

Proposizione 1.3.15 *Siano I, J ideali, allora*

1. $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$;
2. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$;
3. $\mathcal{I}(\mathcal{V}(I) \cup \mathcal{V}(J)) = \mathcal{I}(\mathcal{V}(I)) \cap \mathcal{I}(\mathcal{V}(J))$.

Dimostrazione:

1. $\subseteq$) $\mathcal{V}(I + J) \subseteq \mathcal{V}(I)$ e $\mathcal{V}(I + J) \subseteq \mathcal{V}(J) \Rightarrow \mathcal{V}(I + J) \subseteq \mathcal{V}(I) \cap \mathcal{V}(J)$;
   $\supseteq$) Sia $\alpha \in \mathcal{V}(I) \cap \mathcal{V}(J)$ e $f = i + j \in (I + J) \Rightarrow f(\alpha) = i(\alpha) + j(\alpha) = 0 \Rightarrow \alpha \in \mathcal{V}(I + J)$;
2. Dimostriamo prima che $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$:
   $\subseteq$) $\mathcal{V}(I) \subseteq \mathcal{V}(IJ)$ e $\mathcal{V}(J) \subseteq \mathcal{V}(IJ) \Rightarrow \mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(IJ)$;
   $\supseteq$) Sia $\alpha \in \mathcal{V}(IJ) \Rightarrow \forall ij \in IJ, 0 = (ij)(\alpha) = i(\alpha)j(\alpha) \Rightarrow \alpha \in \mathcal{V}(I) \cup \mathcal{V}(J)$;

   Dimostriamo adesso che $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$:

   $\subseteq$) In generale vale che $I \cap J \supseteq IJ \Rightarrow \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$. Allora, per il punto precedente, si ha $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(I) \cup \mathcal{V}(J)$;
   $\supseteq$) $I \cap J \subseteq I, I \cap J \subseteq J \Rightarrow \mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$.
3. Grazie alle dimostrazioni precedenti la tesi equivale a mostrare che $\mathcal{I}(\mathcal{V}(I \cap J)) = \mathcal{I}(\mathcal{V}(I)) \cap \mathcal{I}(\mathcal{V}(J))$ cioè $\sqrt{(I \cap J)} = \sqrt{I} \cap \sqrt{J}$.
   $\subseteq$) Sia $f \in \sqrt{(I \cap J)} \Rightarrow \exists m \in \mathbb{N}$ tale che $f^m \in I \cap J \Rightarrow f \in \sqrt{I}$ e $f \in \sqrt{J}$;
   $\supseteq$) Sia $f \in \sqrt{I} \cap \sqrt{J} \Rightarrow \exists m, n \in \mathbb{N}$ tali che $f^m \in I, f^n \in J$, allora $f^{m+n} \in I \cap J \Rightarrow f \in \sqrt{(I \cap J)}$.

⋈

Segnaliamo inoltre l'importante seguente proprietà che discende direttamente da quelle appena dimostrate, ma che risulta molto utile per la scomposizione di una varietà in unione di varietà: siano $I, J, L \subseteq \mathbb{K}[x_1, ..., x_n]$, allora

$$\mathcal{V}(I, JL) = \mathcal{V}(I, J) \cup \mathcal{V}(I, L)$$

Proposizione 1.3.16 *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$ ideale, allora I è 0-dimensionale se e solo se la cardinalità di $\mathcal{V}(I)$ è finita.*

Dimostrazione:$\Rightarrow$) $\mathbb{K}[x_1, ..., x_n]/I$ ha dimensione finita m. Per ogni $i = 1, 2..., n$, $1, x_i, ..., x_i^m$ sono linearmente dipendenti su $\mathbb{K}$, dunque esistono $b_0, ..., b_m$ diversi da 0 tali che $g_i = \sum_{j=0}^{m} b_j x_i^j \equiv 0 \pmod I \Rightarrow g_i \in I$. Consideriamo adesso l'ideale $(g_1, ..., g_n) \subseteq I \Rightarrow \mathcal{V}((g_1, ..., g_n)) \supseteq \mathcal{V}(I)$; ma la varietà di $(g_1, ..., g_n)$ è finita (ci sono al più n^m punti) e quindi lo è anche quella di I;
$\Leftarrow$) $\#\mathcal{V}(I)$ finita $\Rightarrow \mathcal{V}(I) = \{p_1, ..., p_s\}$ tali che $p_i \in \mathbb{K}^n$. Scriviamo $p_i = (a_{1,i}, ..., a_{n,i})$ e consideriamo $f_i = \prod_{j=1}^{s}(x_i - a_{i,j})$, allora $\forall i, f_i \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I} \Rightarrow \exists m \in \mathbb{N}$ tale che $f_i^m \in I$. Adesso, gli f_i sono monici e di grado s, quindi anche f_i^m è monico in x_i e quindi I è 0-dimensionale perché esiste per ogni i il polinomio f_i che ha come leading term x_i^{sm}.

⋈

Esempio: Sia $I = (x^2 - x, y^2 - y, x - y)$, è un ideale 0-dimensionale e $\mathcal{V}(I) = \{(0, 0), (1, 1)\}$. Osserviamo che in generale può essere utile calcolare una base di Groebner per capire come è fatta la varietà (nell'esempio avevamo già una base di Groebner: $G = \{y^2 - y, x - y\}$).

Lemma 1.3.17 *Sia $J = (I, fg)$ con I ideale e $f, g \in \mathbb{K}[x_1, ..., x_n]$, allora $\sqrt{J} = \sqrt{(I, f)} \cap \sqrt{(I, g)}$; inoltre, se f e g sono relativamente primi modulo I, allora $J = (I, f) \cap (I, g)$.*

Dimostrazione: Mostriamo la prima parte dell'enunciato: $\sqrt{J} = \sqrt{(I, f)} \cap \sqrt{(I, g)}$

$\subseteq$) Sia $h \in \sqrt{J} \Rightarrow h^m = i + fgk \Rightarrow h^m \in (I, f), h^m \in (I, g) \Rightarrow h \in \sqrt{(I, f)} \cap \sqrt{(I, g)}$;

$\supseteq$) Sia $h \in \sqrt{(I, f)} \cap \sqrt{(I, g)} \Rightarrow h^n = i_1 + fk$, $h^m = i_2 + gl \Rightarrow h^{m+n} = i_1 i_2 + i_1 gl + i_2 fk + fgkl \in J \Rightarrow h \in \sqrt{J}$.

Mostriamo adesso la seconda parte con le ipotesi aggiuntive: $J = (I, f) \cap (I, g)$

$\subseteq$) Vera in generale: sia $h \in J \Rightarrow h = i + fgl \Rightarrow h \in (I, f) \cap (I, g)$;

$\supseteq$) Dato che f, g sono coprimi modulo I possiamo scrivere $1 \equiv af + bg \quad (I)$ per certi $a, b \in A$. Sia allora $h \in (I, f) \cap (I, g)$; dalla relazione precedente si ha $h \equiv h(af + bg) \quad (I)$ e cioè, sviluppando i conti a destra dell'equivalenza, $h \in J$.

⋈

Esempio: $I = (x - y, y^2 - y)$ è un ideale 0-dimensionale, quali sono gli ideali massimali di cui è intersezione? Per il lemma dimostrato $I = (x - y, y) \cap (x - y, y - 1) = (x, y) \cap (x - 1, y - 1)$ che sono ideali massimali. Notiamo inoltre che $\mathcal{V}(I) = \{(0, 0), (1, 1)\} = \mathcal{V}((x, y)) \cup \mathcal{V}((x - 1, y - 1))$.

Definizione 1.33 *Sia A un anello, si definisce **dimensione di A** il massimo n delle lunghezze di catene di ideali primi $P_0 \subsetneq P_1 ... \subsetneq P_n \subsetneq A$. Definiamo inoltre la **dimensione di un ideale I** la dimensione dell'anello A/I, ovvero il massimo delle lunghezze di catene di ideali primi che contengono I, in particolare, se I è massimale, la dimensione è 0.*

Esempio: $\dim \mathbb{Z} = 1$, infatti $(0) = P_0 \subsetneq P_1 = (p) \subsetneq \mathbb{Z}$ con p primo è la lunghezza massima possibile. $\mathbb{K}[x]$ con $\mathbb{K}$ campo ha dimensione 1 poiché tutti gli ideali primi sono massimali e $\mathbb{K}[x]$ è un dominio. $\mathbb{K}[x, y]$ ha dimensione maggiore o uguale a due poiché esiste la catena $(0) \subsetneq (x) \subsetneq (x, y) \subsetneq \mathbb{K}[x, y]$.

Definizione 1.34 *$\mathcal{V}(I)$ varietà di $\mathbb{K}^n$ si dice* ***irriducibile*** *se per ogni V_1, V_2 varietà tali che $\mathcal{V}(I) = V_1 \cup V_2 \Rightarrow \mathcal{V}(I) = V_1$ o $\mathcal{V}(I) = V_2$*

Proposizione 1.3.18 *$\mathcal{V}(I) \subseteq \mathbb{K}^n$ è irriducibile $\Leftrightarrow$ $\mathcal{I}(\mathcal{V}(I))$ è primo.*

Dimostrazione:

$\Rightarrow$) Sia $fg \in \mathcal{I}(\mathcal{V}(I))$ e $V_1 = \mathcal{V}(I) \cap \mathcal{V}(f)$, $V_2 = \mathcal{V}(I) \cap \mathcal{V}(g)$. Notiamo che $f \in \mathcal{I}(V_1)$ e $g \in \mathcal{I}(V_2)$. Sia ora $fg \in \mathcal{I}(\mathcal{V}(I)) \Rightarrow \mathcal{V}(I) = \mathcal{V}(I, fg) = \mathcal{V}(I, f) \cup \mathcal{V}(I, g) = (\mathcal{V}(I) \cap \mathcal{V}(f)) \cup (\mathcal{V}(I) \cap \mathcal{V}(g)) = V_1 \cup V_2$; ma $\mathcal{V}(I)$ è irriducibile e pertanto $\mathcal{V}(I) = V_1$ e quindi f si annulla in $\mathcal{V}(I)$ cioè $f \in \mathcal{I}(V(I))$ oppure $\mathcal{V}(I) = V_2$ e quindi g si annulla in $\mathcal{V}(I)$ cioè $g \in \mathcal{I}(V(I))$;

$\Leftarrow$) Sia $\mathcal{V}(I) = V_1 \cup V_2$ con $V_1 \neq \mathcal{V}(I)$. Voglio dimostrare che $V_2 = \mathcal{V}(I)$ o, analogamente, che $\mathcal{I}(V_2) = \mathcal{I}(\mathcal{V}(I))$. $V_2 \subseteq \mathcal{V}(I) \Rightarrow \mathcal{I}(V_2) \supseteq \mathcal{I}(V(I))$. Dimostriamo adesso l'altro contenimento: dato che $V_1 \subsetneq \mathcal{V}(I) \Rightarrow \mathcal{I}(\mathcal{V}(I)) \subsetneq \mathcal{I}(V_1)$ e pertanto $\exists f \in \mathcal{I}(V_1) - \mathcal{I}(\mathcal{V}(I))$. Sia adesso $g \in \mathcal{I}(V_2)$; visto che $\mathcal{V}(I) = V_1 \cup V_2 \Rightarrow \forall \alpha \in \mathcal{V}(I), fg(\alpha) = 0 \Rightarrow fg \in \mathcal{I}(\mathcal{V}(I))$, ma $\mathcal{I}(\mathcal{V}(I))$ è primo quindi $f \in \mathcal{I}(\mathcal{V}(I))$ o $g \in \mathcal{I}(\mathcal{V}(I))$. Per costruzione $f \notin \mathcal{I}(\mathcal{V}(I)) \Rightarrow g \in \mathcal{I}(\mathcal{V}(I))$, dunque $\mathcal{I}(V_2) \subseteq \mathcal{I}(\mathcal{V}(I))$ che è la tesi.

$\bowtie$

Proposizione 1.3.19 *Ogni varietà affine è unione finita di varietà irriducibili.*

Dimostrazione 1: Sia $\Sigma = \{W \text{ varietà} | \ W \text{ non è unione finita di varietà irriducibili}\}$ ordinata per inclusione $\supseteq$. Supponiamo che Σ sia non vuota e mostriamo che ogni catena ammette maggiorante: sia C la catena $W_0 \supseteq W_1 \supseteq ... W_n \supseteq ...$ e consideriamo la catena associata $\mathcal{I}(W_0) \subseteq ... \subseteq \mathcal{I}(W_n) \subseteq ....$ Abbiamo mostrato che le catene di ideali stabilizzano e pertanto anche la catena delle varietà si stabilizza e dunque esiste il maggiorante. Possiamo dunque applicare il lemma di Zorn e pertanto esiste W elemento minimale. W è riducibile $\Rightarrow W = A \cup B$ con $A \subseteq W$ e $B \subseteq W$. Per ipotesi di minimalità di W, A e B sono unione finita di varietà irriducibili e dunque anche W è unione finita di varietà irriducibili, assurdo;
Dimostrazione 2:(Da vedere il problema della creazione catene infinite): Sia $\mathcal{V}(I_0)$ una varietà affine: se è irriducibile ho finito, altrimenti esistono $\mathcal{V}(I_1)$, $\mathcal{V}(J_1)$ tali che $\mathcal{V}(I_1) \cup \mathcal{V}(J_1) = \mathcal{V}(I_0)$. Di nuovo, se $\mathcal{V}(I_1)$ e $\mathcal{V}(J_1)$ sono entrambi irriducibili ho finito, altrimenti esistono due varietà $\mathcal{V}(I_2)$, $\mathcal{V}(J_2)$ tali che $\mathcal{V}(I_1) = \mathcal{V}(I_2) \cup \mathcal{V}(J_2)$. Procedendo in questo modo e supponendo ogni volta che sia $\mathcal{V}(I_n)$ a essere riducibile si forma la catena

$$\mathcal{V}(I_0) \supseteq \mathcal{V}(I_1) \supseteq ... \supseteq \mathcal{V}(I_n) \supseteq ...$$

la quale, vista come catena di ideali, diventa:

$$\mathcal{I}(\mathcal{V}(I_0)) \subseteq \mathcal{I}(\mathcal{V}(I_1)) \subseteq ... \subseteq \mathcal{I}(\mathcal{V}(I_n)) \subseteq ...$$

Abbiamo dimostrato che ogni catena di ideali in $\mathbb{K}[x_1, ..., x_n]$ ordinata per inclusione si stabilizza, ma allora anche la catena delle varietà si deve stabilizzare e pertanto esisterà $N \in \mathbb{N}$ tale che $\mathcal{V}(I_N) = \mathcal{V}(I_{N+k})$ per ogni $k \in \mathbb{N}$, cioè la varietà $\mathcal{V}(I_N)$ è irriducibile. Dato che ogni catena che parte da $\mathcal{V}(I_0)$ si stabilizza in un numero finito di passi si ha la tesi.

$\bowtie$

Proposizione 1.3.20 *Sia $I = \sqrt{I}$, allora I è intersezione di un numero finito di ideali primi.*

Dimostrazione: Sia I un ideale radicale e sia $\mathcal{V}(I)$ la sua varietà associata. Per la proposizione precedente possiamo scrivere $\mathcal{V}(I) = \mathcal{V}(I_1) \cup ... \cup \mathcal{V}(I_n)$ con $\mathcal{V}(I_i)$ varietà irriducibili. Passando all'ideale della varietà otteniamo allora $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\mathcal{V}(I_1) \cup ... \cup V(I_n)) \Rightarrow \sqrt{I} = \mathcal{I}(\mathcal{V}(I_1)) \cap ... \cap \mathcal{I}(\mathcal{V}(I_n))$. Dato che I è radicale e $\mathcal{I}(\mathcal{V}(I_i)) = P_i$ è primo per ogni i poiché le varietà sono irriducibili allora:

$$I = \bigcap_{i=1}^{n} P_i$$

⋈

Proposizione 1.3.21 *Sia $I \subseteq \mathbb{K}[x_1, ..., x_n]$, $\mathbb{K} = \bar{\mathbb{K}}$, $I = \sqrt{I}$ 0-dimensionale, allora vale:*

1. *$\mathcal{V}(I)$ è finita;*
2. *$I = \bigcap_{i=1}^{s} M_i$ con M_i massimali;*
3. *$dim(\mathbb{K}[x_1, ..., x_n]/I) = \#\mathcal{V}(I) = s$.*

Dimostrazione:

1. Già vista;
2. Per il punto precedente $\mathcal{V}(I)$ è finita e pertanto $\mathcal{V}(I) = \{p_1, ..., p_s\}$. Possiamo dunque scrivere:
   $$\mathcal{V}(I) = \{p_1\} \cup ... \cup \{p_s\} = \mathcal{V}(M_1) \cup ... \cup \mathcal{V}(M_s)$$
   dove gli $M_i = \mathcal{I}(p_i)$ sono massimali per la caratterizzazione fatta. Passando dunque all'ideale delle varietà si ottiene:
   $$I = \sqrt{I} = \mathcal{I}(\mathcal{V}(I)) = M_1 \cap ... \cap M_s = \bigcap_{i=1}^{s} M_i$$
3. $\mathbb{K}[x_1, ..., x_n]/I = \mathbb{K}[x_1, ..., x_n]/(\bigcap_{i=1}^{m} M_i) = \mathbb{K}[x_1, ..., x_n]/M_1 \times ... \times \mathbb{K}[x_1, ..., x_n]/M_s = \mathbb{K} \times ... \times \mathbb{K} = \mathbb{K}^s$ dove le ultime due uguaglianze seguono dal teorema del resto cinese per anelli e dalle proprietà di spazio vettoriale. Dunque $\dim(\mathbb{K}[x_1, ..., x_n]/I) = s = \#\mathcal{V}(I)$.

⋈

Capitolo 2

A-Moduli

2.1 Definizioni e prime proprietà

Definizione 2.1 *Sia A anello commutativo con unità, un insieme M si dice* ***A-modulo*** *se:*

1. *$(M, +)$ è un gruppo;*
2. *Esiste una funzione $" \cdot " : A \times M \to M$ tale che $(a, m) \to am$ tale che $\forall a, b \in A, m, n \in M$:*
   - $(a + b)m = am + bm$;
   - $a(m + n) = am + an$;
   - $a(bm) = (ab)m = abm$;
   - $1_A m = m$.

Osservazione: In un A-modulo convivono lo zero di A e lo zero di M; in particolare si ha che $0_A m = 0_M$ e $a0_M = 0_M$ per ogni $a \in A$ e $m \in M$.

Osservazione: Se A è un campo, allora un A-modulo è uno spazio vettoriale. Possiamo inoltre vedere A come A-modulo su se stesso prendendo $M = A$. Se $B \subseteq A$, A è anche un B-modulo.

Esempio: Se $A = \mathbb{Z}$, gli $\mathbb{Z}$-moduli sono i gruppi abeliani. $A[x]$ con A anello, è un A-modulo.

Definizione 2.2 *Sia M A-modulo, $N \subseteq M$ si dice* ***sottomodulo*** *se N è un sottogruppo di $(M, +)$ e $\forall a \in A, n \in N$ si ha che $an \in N$.*

Osservazione: In ogni A-modulo M, $\{0\}$ e M sono sottomoduli. Se $M = A$, allora i sottomoduli di A sono i suoi ideali.

Definizione 2.3 *Sia M A-modulo e $I \subseteq A$ ideale, definiamo*

$$IM = \Big\{ \sum_{i=1}^{n} a_i m_i | a_i \in I, m_i \in M \Big\} \subseteq M$$

Notiamo che IM è un sottomodulo di M.

Definizione 2.4 *Sia M A-modulo, $S \subseteq M$, definiamo il più piccolo sottomodulo generato da S:*

$$< S >= \Big\{ \sum_{i=1}^{n} a_i s_i | a_i \in A, s_i \in S \Big\}$$

Definizione 2.5 *Sia M A-modulo, un insieme $S \subseteq M$ si dice* ***insieme di generatori per M*** *se $\forall m \in M, \exists a_1, ..., a_k \in A$ e $m_1, ..., m_k \in S$ tali che $m = \sum_{i=1}^{k} a_i m_i$. Se S ha cardinalità finita, diremo che M è* ***finitamente generato****.*

Definizione 2.6 *Sia M A-modulo, un insieme $S \subseteq M$ si dice* ***libero*** *o che gli elementi di S sono* ***linearmente indipendenti*** *se $\forall a_1, ..., a_k \in A$ e $\forall m_1, ..., m_k \in S$ tali che $\sum_{i=1}^{k} a_i m_i = 0 \Rightarrow a_i = 0 \; \forall i$.*

Definizione 2.7 *Sia M A-modulo, un insieme $S \subseteq M$ si dice* ***base di M*** *se S è libero e genera M.*

Definizione 2.8 *Sia M A-modulo, M si dice* ***libero*** *se ammette una base.*

Definizione 2.9 *Sia M A-modulo, M si dice* ***modulo ciclico*** *se esiste $m \in M$ tale che $< m >= M$.*

ESEMPIO: $A[x]$ con A anello, non è finitamente generato; $\mathbb{Z}$ come $\mathbb{Z}$-modulo è generato ad esempio da: $\{1\}$, $\{2, 3\}$, $\{2, 6, 9\}$, si nota però che solo $\{1\}$ è una base e che solo $\{2, 6, 9\}$ non è un insieme di generatori minimale.

OSSERVAZIONE: Non sempre esiste una base di un A-modulo: consideriamo ad esempio $\mathbb{Z}_n$ come $\mathbb{Z}$-modulo, ogni elemento non è linearmente indipendente: basta moltiplicarlo per n. Se invece consideriamo $\mathbb{Z}_n$ come $\mathbb{Z}_n$-modulo, allora $\{1\}$ è una base. In generale avremmo che ogni anello A è libero come A-modulo. Anche

$$A^n = A \times A \times ... \times A$$

è un A-modulo libero e una base è costituita da $e_1 = (1, 0, ..., 0), ..., e_n = (0, ..., 0, 1)$. Invece $\mathbb{Q}$ come $\mathbb{Z}$-modulo non è libero, infatti un elemento da solo non basta per generare e se ci sono due elementi nella base, questi non possono essere linearmente indipendenti.

Definizione 2.10 *Siano M, N A-moduli, $f : M \to N$ si dice* ***omomorfismo di A-moduli*** *se*

- $f(m + n) = f(m) + f(n) \quad \forall m, n \in M$
- $f(am) = af(m) \quad \forall a \in A, m \in M$

ESEMPIO: $g : \mathbb{Z} \to \mathbb{Z}$ tale che $g(1) = 2$ è un omomorfismo di $\mathbb{Z}$-moduli; ricordiamo invece che esiste un unico morfismo di anelli da $\mathbb{Z}$ in $\mathbb{Z}$ che è l'identità.

Definizione 2.11 *Siano M, N A-moduli, $f, g : M \to N$ omomorfismi di A-moduli, definiamo le operazioni:*

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

Prodotto esterno: $(af)(m) = a(f(m)) \; \forall a \in A, m \in M$

Dotato di tali operazioni $Hom_A(M, N)$ è un A-modulo.

OSSERVAZIONE: Se M e N sono A-moduli e $f : M \to N$ omomorfismo di A-moduli, allora $Kerf$ è un sottomodulo di M e Imf è un sottomodulo di N.

Definizione 2.12 *Sia M A-modulo e N un suo sottomodulo, definiamo nel quoziente M/N il prodotto $a(m + N) = am + N$. Con la somma indotta dalla struttura delle classi laterali e con il prodotto appena definito M/N è un A-modulo.*

Notiamo che il prodotto è ben definito: se $m \equiv m_1\ (N) \Rightarrow am = a(m_1 + n) = am_1 + an \equiv am_1\ (N)$.

Definizione 2.13 *Siano M, N A-moduli, definiamo $CoKerf = N/Imf$.*

Proposizione 2.1.1 (Primo teorema di omomorfismo) *Siano M, N A-moduli, $f : M \to N$ omomorfismo di A-moduli allora $Imf \cong M/Kerf$.*

Proposizione 2.1.2 (Secondo teorema di omomorfismo) *Siano $N \subseteq M \subseteq P$ A-moduli, allora $P/M \cong (P/N)/(M/N)$.*

Operazioni tra sottomoduli: Siano $M_1, M_2, ...$ sottomoduli di M A-modulo, definiamo le seguenti operazioni:

Somma interna: $\sum_i M_i = \{\sum_i m_i | m_i \neq 0$ per un numero finito di indici e $m_i \in M_i\}$;

Intersezione: $\bigcap_i M_i = \{m | m \in M_i \quad \forall i\}$;

Colon: $(M_1 : M_2) = \{a \in A | aM_2 \subseteq M_1\}$ (Non è un sottomodulo, ma un ideale);

Annullatore: $Ann(M) = (0 : M)$.

Proposizione 2.1.3 *Siano M_1, M_2 sottomoduli di M A-modulo, allora $(M_1+M_2)/M_1 \cong M_2/(M_1 \cap M_2)$*

Dimostrazione: Consideriamo $\varphi : M_2 \xrightarrow{i} (M_1 + M_2) \xrightarrow{\pi} (M_1 + M_2)/M_1$. $\varphi = \pi \circ i$ è un omomorfismo, è banalmente suriettiva, e $Ker\varphi = (M_1 \cap M_2)$.

⋈

Proposizione 2.1.4 *Sia M un A-modulo e $N, M_1, M_2 \subseteq M$ sottomodulo, valgono le seguenti proprietà:*

1. *$Ann(M/N) = (N : M)$;*
2. *$Ann(M_1 + M_2) = Ann(M_1) \cap Ann(M_2)$;*

Dimostrazione:

1. $Ann(M/N) = (0 : M/N)$, dunque $a \in (0 : M/N) \Leftrightarrow a(m + N) = 0\ \forall m \in M \Leftrightarrow am \in N\ \forall m \in M \Leftrightarrow a \in (N : M)$;
2. $\subseteq$): Segue dal fatto che $M_1 \subseteq M_1 + M_2$ e $M_2 \subseteq M_1 + M_2$;
   $\supseteq$): $a \in Ann(M_1) \cap Ann(M_2) \Rightarrow a(m_1 + m_2) = am_1 + am_2 = 0\ \forall m_1 \in M_1, m_2 \in M_2 \Rightarrow a \in Ann(M_1 + M_2)$;

⋈

Definizione 2.14 *Sia A anello, $I \subseteq A$ ideale, M un A-modulo; M/IM è un A/I-**modulo** con il prodotto esterno: $(a + I)(m + IM) = am + IM$.*

Notiamo che il prodotto è ben definito poiché, se $a = a_1 + I, m = m_1 + IM$ allora $am = (a_1 + i)(m_1 + jn) = (a_1m_1 + ijm_1n + a_1jn + im_1) \equiv a_1m_1\ (IM)$.

Proposizione 2.1.5 *Sia M un A-modulo libero e $\mathcal{B}$ una sua base finita, allora tutte le basi di M hanno la stessa cardinalità.*

Dimostrazione: Sia $\mathcal{B} = \{m_1, ..., m_k\}$ base di M, prendiamo $I \subseteq A$ ideale massimale (esiste sempre per il lemma di Zorn) e consideriamo M/IM come A/I modulo. Essendo A/I un campo, M/IM è uno spazio vettoriale, ci basta dunque dimostrare che questo ha dimensione k per avere la tesi grazie alla proprietà di spazio vettoriale. Consideriamo la proiezione: $\pi : M \to M/IM$: l'insieme $\{\bar{m_1}, ..., \bar{m_k}\}$ genera l'immagine poiché $\forall m \in M, m = \sum_{i=1}^{k} a_i m_i$ per certi $a_i \in A$ e $\pi(m) = \sum_{i=1}^{k} \bar{a_i}\bar{m_i}$. Resta da mostrare che gli $\bar{m_i}$ sono linearmente indipendenti: sia $\sum_{i=1}^{k} \bar{a_i}\bar{m_i} = \sum_{i=1}^{k}(a_i + I)(m_i + IM) = 0 \Rightarrow \sum_{i=1}^{k} a_i m_i \in IM \Rightarrow \exists j \in I, m \in M$ tali che $\sum_{i=1}^{k} a_i m_i = jm = \sum_{i=1}^{k} b_i m_i$ con i $b_i \in I$, allora $\sum_{i=1}^{k}(a_i - b_i)m_i = 0$ e dunque $a_i = b_i \Rightarrow a_i + I = I$ che era la nostra tesi.

⋈

Grazie alla proposizione precedente siamo in grado di dare la seguente:

Definizione 2.15 *Se M è un A-modulo libero, e $\mathcal{B} = \{m_1, ..., m_k\}$ è una base di M allora k viene detto **rango del modulo**. In particolare il rango del modulo corrisponde alla dimensione dello spazio vettoriale M/IM a coefficienti in A/I con $I \subseteq A$ ideale massimale.*

Proposizione 2.1.6 *Sia M un A-modulo, se esiste una base infinita C, allora tutte le basi di M sono infinite.*

Dimostrazione: Supponiamo che esista $\mathcal{B} = \{m_1, ..., m_k\}$ base finita di M; allora per ogni i posso scrivere $m_i = \sum_{j=1}^{t_i} a_{i,j}c_{i,j}$ con $c_{i,j} \in C$. L'insieme $T = \{c_{1,1}, ..., c_{1,t_1}, c_{2,1}, ..., ..., c_{k,t_k}\}$ è contenuto in C ed è un insieme di generatori per M. Sia ora $c \in C - T \Rightarrow c = \sum_{i,j} b_{i,j}c_{i,j}$ con i $b_{i,j}$ non tutti nulli e pertanto $c - \sum_{i,j} b_{i,j}c_{i,j} = 0$, ma questo è assurdo poiché $\{T, c\} \subseteq C$ è un insieme di elementi linearmente dipendenti.

⋈

Proposizione 2.1.7 *Sia M A-modulo libero finitamente generato, allora ogni insieme di generatori ha cardinalità maggiore uguale al rango.*

Dimostrazione: Supponiamo che $rkM = k$ e che esista un insieme di generatori G di cardinalità strettamente minore di k. Allora, procedendo come sopra, M/IM come spazio vettoriale dovrebbe avere dimensione strettamente minore di k, ma questo è assurdo dalla definizione di rango.

⋈

Proposizione 2.1.8 *Sia M A-modulo, allora $Hom_A(A, M) \cong M$ come A-moduli.*

Dimostrazione: Essendo A un anello, ogni omomorfismo è definito da dove viene mandato 1, sia dunque $f_m : A \to M$ l'omomorfismo tale che $f_m(1) = m$, definiamo quindi la mappa $F : M \to Hom_A(A, M)$ tale che $F(m) = f_m$. Si verifica facilmente che è un morfismo di A-moduli iniettivo e suriettivo.

⋈

Esercizio: Dimostrare che

1. $Hom_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$;
2. $Hom_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \cong 0$;
3. $Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) \cong 0$;
4. $Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Q}/\mathbb{Z}) \ncong 0$;

Soluzione:

1. Segue dalla proposizione precedente;

2. Prendiamo $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ e supponiamo $\varphi(1) = m$. In $\mathbb{Q}$ possiamo scrivere $1 = p/p \; \forall p \in \mathbb{Z}$, dunque $m = \varphi(p/p) = p\varphi(1/p) \Rightarrow p|m \; \forall p \in \mathbb{Z} \Rightarrow m = 0$, in cui la seconda uguaglianza è data dalla $\mathbb{Z}$-linearità. Abbiamo mostrato che φ vale zero su tutto $\mathbb{Z}$, resta da dimostrare che $\varphi = 0$ anche su $\mathbb{Q}$: per ogni $a/b \in \mathbb{Q}$, b non nullo, vale $b\varphi(a/b) = \varphi(a) = 0 \Rightarrow \varphi(a/b) = 0$ essendo $b \neq 0$ e $\mathbb{Z}$ un dominio;

3. Se $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z})$ allora $\varphi(0) = 0$ e $\varphi(1) = m \in \mathbb{Z}$, ma $2m = \varphi(1+1) = \varphi(0) = 0 \Rightarrow m = 0$;

4. Risulta ben definito l'omomorfismo non nullo $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Q}/\mathbb{Z})$ tale che $\varphi(0) = 0 + \mathbb{Z}$ e $\varphi(1) = 1/2 + \mathbb{Z}$, infatti $\varphi(1+1) = 1/2 + 1/2 + \mathbb{Z} = 0 + \mathbb{Z}$.

Definizione 2.16 *Siano $\{M_i\}_{i \in H}$ una famiglia di A-moduli; definiamo* ***somma diretta di A-moduli****:*

$$\bigoplus_{i \in H} M_i = \{(m_i)_{i \in H} |\; m_i \neq 0 \text{ per un numero finito di indici}\}$$

Nelle stesse ipotesi, definiamo anche il ***prodotto diretto di A-moduli****:*

$$\prod_{i \in H} M_i = \{(m_i)_{i \in H}\}$$

Osservazione: Nelle notazioni precedenti, se H è finito, il prodotto diretto è uguale alla somma diretta.

Proposizione 2.1.9 *Sia M un A-modulo libero, allora $M \cong \bigoplus_i M_i$ con $M_i \cong A$ per ogni i.*

Dimostrazione: Consideriamo una base $\mathcal{B} = \{b_1, ..., b_n\}$ di M (nel caso in cui la base sia infinita la dimostrazione è analoga); per ogni $m \in M$, $m = \sum_{i=1}^{n} a_i b_i$ con gli $a_i \in A$; sia allora

$$\varphi : M \to < b_1 > \oplus ... \oplus < b_n >$$

tale che $\varphi(m) = (a_1 b_1, ..., a_n b_n)$. Si verifica facilmente che φ è un isomorfismo di A-moduli e, dato che $< b_i > \cong A$ tramite l'isomorfismo $f :< b_i > \to A$, $f(ab_i) = a$, $M \cong A^n$.

⋈

Osservazione: Ogni A-modulo M finitamente generato è quoziente di un A-modulo libero. Supponiamo che M abbia un insieme di generatori $\{m_1, ..., m_k\}$, consideriamo $A^k = A \times A \times ... \times A$ (che è un A-modulo libero) e la mappa $\varphi : A^k \to M$ tale che $\varphi(a_1, ..., a_k) = \sum_{i=1}^{k} a_i m_i$. Allora $M \cong A^k / Ker\varphi$. Vale anche il viceversa, ovvero che se M è quoziente di A^n, allora M è finitamente generato.

Osservazione: Supponiamo M A-modulo di rango k, e $f : M \to M$ un endomorfismo, allora non è vero che se f è iniettivo, allora f è suriettivo: consideriamo infatti che $f : \mathbb{Z} \to \mathbb{Z}$ tale che $f(1) = 2$; f è chiaramente iniettivo, ma non è suriettivo. Dimostreremo invece che vale il viceversa, e cioè che, se f è suriettivo, allora è anche iniettivo.

Definizione 2.17 *Sia $P \in M_n(A)$ con A anello, allora si definisce* ***aggiunta di T*** *la matrice $P^* \in M_n(A)$ tale che*

$$[P^*]_{i,j} = (-1)^{i+j} det(P^T_{i,j})$$

dove con $P^T_{i,j}$ si intende il complemento algebrico di P^T rispetto alla riga i e alla colonna j, cioè la matrice P^T privata della riga i e della colonna j:

$$P^* = \begin{bmatrix} (-1)^2 det(P^T_{1,1}) & (-1)^3 det(P^T_{1,2}) & ... & ... & (-1)^{1+n} det(P^T_{1,n}) \\ (-1)^3 det(P^T_{2,1}) & ... & ... & ... & (-1)^{2+n} det(P^T_{2,n}) \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ (-1)^{n+1} det(P^T_{n,1}) & ... & ... & ... & (-1)^{2n} det(P^T_{n,n}) \end{bmatrix}$$

OSSERVAZIONE: Se la matrice è a coefficienti in un anello, la matrice aggiunta esiste sempre poiché dipende soltanto da somme e prodotti che sono operazioni ben definite.

ESEMPIO: Sia $P \in M_3(\mathbb{R})$ tale che:

$$P = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix} \qquad P^T = \begin{bmatrix} 3 & 0 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

allora la sua matrice aggiunta è:

$$P^* = \begin{bmatrix} (-1)^2 det \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} & (-1)^3 det \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} & (-1)^4 det \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} \\ (-1)^3 det \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} & (-1)^4 det \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} & (-1)^5 det \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \\ (-1)^4 det \begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix} & (-1)^5 det \begin{pmatrix} 3 & 0 \\ 1 & 0 \end{pmatrix} & (-1)^6 det \begin{pmatrix} 3 & 0 \\ 1 & 3 \end{pmatrix} \end{bmatrix} = \begin{bmatrix} 6 & -2 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 9 \end{bmatrix}$$

Proposizione 2.1.10 *Sia $P \in M_n(A)$ con A anello e P^* la sua aggiunta, allora $P^*P = PP^* = det(P)I$.*

Dimostrazione: Dobbiamo verificare che per ogni h, k $[P^*P]_{h,k} = det(P)[I]_{h,k}$ (l'altra uguaglianza si dimostra in maniera analoga). Distinguiamo due casi:

$h = k$ $[P^*P]_{h,h} = \sum_{i=1}^n (-1)^{h+i} det(P^T_{h,i})[P]_{i,h} = \sum_{i=1}^n (-1)^{h+i} det(P^T_{h,i})[P^T]_{h,i} = det(P^T) = det(P)$;

$h \neq k$ $[P^*P]_{h,k} = \sum_{i=1}^n (-1)^{h+i} det(P^T_{h,i})[P]_{i,k} = \sum_{i=1}^n (-1)^{h+i} det(P^T_{h,i})[P^T]_{k,i} = 0$ poiché questo è lo sviluppo secondo la riga h-esima di una matrice ottenuta da P^T sostituendo alla riga h-esima, la riga k-esima e che quindi ha due righe uguali.

⋈

ESEMPIO: Consideriamo P e P^* come nell'esempio precedente, allora $det(P) = 18$ e

$$P^*P = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 6 & -2 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 9 \end{bmatrix} = \begin{bmatrix} 18 & 0 & 0 \\ 0 & 18 & 0 \\ 0 & 0 & 18 \end{bmatrix} = det(P) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Teorema 2.1.11 (Teorema di Hamilton-Cayley) *Sia M A-modulo finitamente generato e $I \subseteq A$ ideale, sia inoltre $f : M \to M$ endomorfismo, se $f(M) \subseteq IM$, allora esistono $a_0, ..., a_{n-1} \in I$ tale che $f^n + a_{n-1}f^{n-1} + ... + a_1 f^1 + a_0 f^0 = 0$*

Dimostrazione: Sia $G = \{m_1, ..., m_n\}$ generatori, allora $f(m_i) = \sum_{j=1}^n c_{i,j} m_j$ con $c_{i,j} \in I$ poiché $f(M) \subseteq IM$. Possiamo riscrivere allora $\forall i \sum_{j=1}^n (\delta_{i,j} f - c_{i,j}) m_j = 0$ dove $\delta_{i,j}$ è il delta di Kronecker

e $\delta_{i,j}f - c_{i,j}$ sono funzioni applicate agli m_j. Possiamo dunque scrivere la matrice associata alla scrittura:

$$\begin{pmatrix} f-c_{1,1} & ... & ... & -c_{1,n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ -c_{n,1} & ... & ... & f-c_{n,n} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Chiamiamo T questa matrice a coefficienti in $I[f]$ e moltiplichiamola a sinistra per la sua aggiunta T^*. Grazie alla proposizione appena dimostrata otteniamo la seguente uguaglianza:

$$T^*T \begin{pmatrix} m_1 \\ \vdots \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} det(T) & 0 & ... & 0 \\ 0 & det(T) & & \vdots \\ \vdots & & & \vdots \\ 0 & ... & ... & det(T) \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Ma allora $det(T)(m_i) = 0$ per ogni i (e quindi per ogni $m \in M$ poiché gli m_i generano M per ipotesi). Dato che $det(T)$ è una funzione polinomiale dei coefficienti della matrice, posso scrivere $det(T) = f^n + a_{n-1}f^{n-1} + ... + a_1f^1 + a_0f^0$ con gli $a_i \in I$; $det(T)$ è pertanto la funzione cercata.

⋈

Corollario 2.1.12 (Lemma di Nakayama) *Sia M A-modulo finitamente generato, $I \subseteq A$ ideale, $M = IM$, allora $\exists a \in A$, $a \equiv 1(I)$ tale che $aM = 0$.*

Dimostrazione: Consideriamo $f : M \to M$, $f = id$, allora siamo nelle ipotesi del teorema precedente, dunque esistono $a_0, ..., a_{n-1}$ tali che $id^n + \sum_{i=0}^{n-1} a_i id^i = 0$ come omomorfismo; vedendolo come omomorfismo di moltiplicazione si ha $1 + \sum_{i=0}^{n-1} a_i = a \in A$, $a \equiv 1$ (I) e $am = 0$ per ogni m.

⋈

Corollario 2.1.13 *Sia M A-modulo finitamente generato, $I \subseteq \mathcal{J}(A)$ ideale tale che $IM = M$, allora $M = 0$.*

Dimostrazione: Per il lemma di Nakayama $\exists a \in A$ tale che $aM = 0$ e $a \equiv 1 \quad (I)$; allora $(a-1) \in I$, ma $I \subseteq \mathcal{J}(A)$ e pertanto, per la caratterizzazione del Jacobson, si ha che $[(a-1)+1] \in A^*$ e dunque $aM = 0 \Rightarrow M = 0$.

⋈

Corollario 2.1.14 *Sia M A-modulo finitamente generato, $I \subseteq \mathcal{J}(A)$ ideale, $N \subseteq M$ sottomodulo tale che $M = IM + N$, allora $M = N$.*

Dimostrazione: Vogliamo dimostrare che $I(M/N) = (M/N)$ così da poter usare il corollario precedente e concludere che $M/N = 0$ e pertanto $M = N$. Sia $S = \{m_1, ..., m_n\}$ un insieme di generatori di M, allora $I(M/N) = \{\sum_{i=1}^n a_i(m_i + N) |\ a_i \in I\} = \{(\sum_{i=1}^n a_i m_i) + N |\ a_i \in I\} = (IM + N)/N = M/N$.

⋈

Proposizione 2.1.15 *Sia M A-modulo finitamente generato, A locale, I massimale; siano $m_1, ..., m_k$ tali che $\pi(m_1), ..., \pi(m_k)$ è una base di M/IM come A/I-modulo (con π proiezione canonica); allora $m_1, ..., m_k$ generano M.*

Dimostrazione: Sia $N =< m_1, ..., m_k >\subseteq M$, vorremmo far vedere che vale l'uguaglianza: consideriamo

$$\varphi : N \xrightarrow{i} M \xrightarrow{\pi} M/IM$$

dove i è l'immersione canonica e π è la proiezione. La funzione $\varphi = \pi \circ i$ è suriettiva per costruzione quindi $N = M + IM \Rightarrow M = N + IM$. Dato che $I = \mathcal{J}(A)$ posso applicare il corollario precedente ottenendo $M = N$, che è la tesi.

$\bowtie$

Proposizione 2.1.16 *Sia M A-modulo finitamente generato, $f : M \to M$ un endomorfismo suriettivo, allora f è iniettivo.*

Dimostrazione: Definiamo su M la struttura di $A[x]$ modulo; in particolare definiamo il prodotto esterno: sia $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, allora $p(x)m = \sum_{i=0}^{n} a_i f^i(m)$ (in sostanza $xm = f(m)$). Adesso, per la suriettività si che $M = Imf$ e

$$M = Imf = \{f(m) |\ m \in M\} = \{xm |\ m \in M\} = (x)M$$

e pertanto (x) è tale che $(x)M = M$. Possiamo quindi applicare il lemma di Nakayama e dunque esiste $p(x) \in A[x]$ tale che $p(x) \equiv 1 \quad (x$ (ovvero $p(x) = 1 + xq(x))$ e $p(x)M = 0$. Sia ora $m \in Kerf$, per costruzione $p(x)m = 0$ e dunque $0 = (1 + xq(x))m = m + q(x)f(m) = m$.

$\bowtie$

Proposizione 2.1.17 *Sia M A-modulo libero di rango n, allora ogni insieme di generatori di M è una base di M.*

Dimostrazione: Sia $S = \{m_1, ..., m_n\}$ un insieme di generatori di M e consideriamo la mappa:

$$M \xrightarrow{f} A^n \xrightarrow{g} M$$

dove f è un isomorfismo (esiste per proposizioni precedenti) e g tale che $g((a_1, ..., a_n)) = \sum_{i=1}^{n} a_i m_i$. La funzione $f \circ g$ è suriettiva poiché g e f sono suriettive e, per la proposizione precedente, è anche iniettiva $\Rightarrow f \circ g$ è isomorfismo e, dato che lo è anche f, g è isomorfismo. Quindi $Kerg = 0$ e pertanto gli m_i sono linearmente indipendenti.

$\bowtie$

Proposizione 2.1.18 *Siano M un A-modulo, $N \subseteq M$ un sottomodulo finitamente generato, $I \subseteq \mathcal{J}(A)$ un ideale di A, e $\varphi : M \to N$ un omomorfismo di A-moduli. Se $\bar{\varphi} : M/IM \to N/IN$ è surgettivo allora anche φ è surgettivo.*

Dimostrazine: Abbiamo la seguente situazione:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle \pi_M}\downarrow & & \downarrow{\scriptstyle \pi_N} \\ M/IM & \xrightarrow{\bar{\varphi}} & N/IN \end{array}$$

Grazie alla surgettività di $\bar{\varphi}$ $\forall n \in N\ \exists m \in M$ tale che $n + IN = \bar{\varphi}(m + IM) = \varphi(m) + IN$, in cui l'ultima uguaglianza è conseguenza del diagramma. Abbiamo dunque $N = Im\varphi + IN$ e, per Nakayama, ciò implica $N = Im\varphi$, ovvero φ è surgettiva.

$\bowtie$

Definizione 2.18 *Sia $\{M_i\}_{i\in H}$ una famiglia di A-moduli e $\{f_i\}_{i\in H}$ una famiglia di omomorfismi tali che*

$$... \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} ...$$

allora la successione si dice ***esatta in*** *M_i se $Kerf_{i+1} = Imf_i$. Inoltre la successione si dice* ***esatta*** *se è esatta per ogni M_i. La successione si dice* ***complesso*** *se $Kerf_{i+1} \supseteq Imf_i$ per ogni i. In particolare, una successione del tipo:*

$$0 \longrightarrow M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \longrightarrow 0$$

esatta in ogni M_i prende il nome di ***successione esatta corta****.*

Dati M, N, P A-moduli, riportiamo i seguenti fatti di immediata dimostrazione che rappresentano dei casi particolari di successioni esatte:

1. $0 \longrightarrow M \xrightarrow{f} N$ è esatta $\Leftrightarrow$ f è iniettiva;
2. $N \xrightarrow{g} P \longrightarrow 0$ è esatta $\Leftrightarrow$ g è suriettiva;
3. $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ è esatta corta $\Leftrightarrow$ f iniettiva, g suriettiva e $P = CoKerf$.

Lemma 2.1.19 *Sia M A-modulo, M_1, M_2 sottomoduli di M, allora la successione:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 \cap M_2 & \xrightarrow{f} & M_1 \oplus M_2 & \xrightarrow{g} & M_1 + M_2 & \longrightarrow & 0 \\ & & m & \longrightarrow & (m, -m) & & & & \\ & & & & (m_1, m_2) & \longrightarrow & (m_1 + m_2) & & \end{array}$$

è esatta corta.

Dimostrazione: Dimostriamo l'esattezza nei tre nodi:

f **iniettiva)** Siano $a, b \in M_1 \cap M_2$ tali che $f(a) = f(b) \Rightarrow (a, -a) = (b, -b) \Rightarrow (a - b, b - a) = (0, 0) \Rightarrow a = b$;

g **suriettiva)** Sia $m \in M_1 + M_2 \Rightarrow m = m_1 + m_2$. Mi basta scegliere la coppia $(m_1, m_2) \in M_1 \oplus M_2$ per avere la tesi;

Imf = Ker$g$) Sia $(m_1, m_2) \in Kerg \Rightarrow m_1 + m_2 = 0 \Rightarrow m_1 = -m_2 \Rightarrow (m_1, m_2) \in Imf$. Viceversa sia $(m, -m) \in Imf \Rightarrow g(m, -m) = 0 \Rightarrow (m, -m) \in Kerg$.

$\bowtie$

Osservazione: Grazie al lemma dimostrato possiamo mostrare che un modulo M è somma diretta di due suoi sottomoduli M_1, M_2 verificando solamente che $M_1 \cap M_2 = 0$ e $M_1 + M_2 = M$.

Osservazione: Data la somma diretta di A-moduli $M \oplus N$ possiamo sempre costruire la successione esatta corta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & M \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \\ & & m & \longrightarrow & (m, 0) & & & & \\ & & & & (m, n) & \longrightarrow & n & & \end{array}$$

Non è vero il viceversa, ovvero, se abbiamo una successione esatta corta, non è detto che il nodo centrale sia somma diretta degli altri due moduli; ad esempio

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_2 & \xrightarrow{\cdot 2} & \mathbb{Z}_4 & \xrightarrow{\pi} & \mathbb{Z}_2 & \longrightarrow & 0 \\ & & 1 & \longrightarrow & 2 & & & & \\ & & & & 1 & \longrightarrow & 1+(2) & & \end{array}$$

Definizione 2.19 *Data la successione esatta corta*

$$0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$$

*se $N \cong M \oplus P$ si dice che **la successione spezza**.*

Teorema 2.1.20 *Data la successione esatta corta*

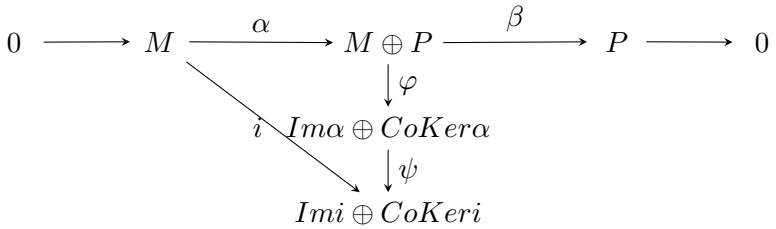
$$0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$$

i seguenti fatti sono equivalenti:

1. *La successione spezza;*
2. *$\exists r : N \to M$ tale che $r \circ \alpha = id_M$ (r è detta **retrazione**);*
3. *$\exists s : P \to N$ tale che $\beta \circ s = id_P$ (s è detta **sezione**).*

Dimostrazione:

$1 \Rightarrow 2$) Sia $N = M \oplus P$: se α è l'immersione canonica, allora la tesi segue banalmente scegliendo $r = \pi$ proiezione sulla prima coordinata. Se invece α non è l'immersione consideriamo il seguente grafico:



Dove φ e ψ sono isomorfismi di A-moduli poiché $M \cong Im\alpha \cong Imi$ e $P \cong CoKer\alpha \cong CoKeri$ per ipotesi. Allora definiamo $r : N \to M$ come $r = \pi \circ \psi \circ \varphi$ ed r è una retrazione.

$1 \Rightarrow 3$) Costruzione analoga alla precedente.

$2 \Rightarrow 1$) Sia $n \in N$, riscriviamolo come $n = (n - \alpha(r(n))) + \alpha(r(n))$. Chiamiamo $L =< n - \alpha(r(n)) >$, vogliamo provare che $N \cong L \oplus Im\alpha$ e che $L \cong P$ e $Im\alpha \cong M$. Per quanto riguarda la somma diretta, grazie al lemma, ci basta dimostrare che $L \cap Im\alpha = 0$ (la condizione $L + Im\alpha = N$ è ovvia): sia $l \in L \cap Im\alpha \Rightarrow n - \alpha(r(n)) = l = \alpha(m)$ per certi $n \in N, m \in M$. Applicando r a entrambi i membri si ottiene $0 = m$ e pertanto l'intersezione è banale. $M \cong Im\alpha$ poiché α è iniettiva. Infine mostriamo che $L \cong P$ tramite l'isomorfismo $\beta_{|_L}$: $Ker\beta_{|_L} = L \cap Im\alpha = 0$, per quanto riguarda la surgettività, siano $p \in P$ e $n \in N$ tale che $\beta(n) = p$ (esiste poiché β è suriettiva), allora $p = \beta(n) = \beta(n - \alpha(r(n)) + \alpha(r(n))) \Rightarrow \beta_{|_L}(n - \alpha(r(n))) = p$;

$3 \Rightarrow 1$) Svolgimento analogo al precedente.

⋈

Lemma 2.1.21 (Lemma del serpente) *Sia dato il seguente grafico:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow[f_1]{} & M_1 & \xrightarrow[g_1]{} & P_1 & \longrightarrow & 0 \end{array}$$

con successioni di A-moduli esatte e ogni diagramma commutativo. Se due qualsiasi tra α, β, γ sono isomorfismi, allora anche il terzo è isomorfismo.

Dimostrazione: Dimostriamo che se α, β sono isomorfismi, allora lo è anche γ (le altre dimostrazioni sono analoghe).

γ **iniettiva:** Sia $p \in P$ tale che $\gamma(p) = 0$. Per la suriettività di g, $\exists m \in M$ tale che $g(m) = p$. Dato che β è un isomorfismo e i diagrammi commutano si ha che $\gamma(g(m)) = g_1(\beta(m)) = 0 \Rightarrow \beta(m) \in Kerg_1 = Imf_1 \Rightarrow \exists n_1 \in N_1$ tale che $f_1(n_1) = \beta(m)$, ma allora, dato che α è isomorfismo $\exists n \in N$ tale che $\alpha(n) = n_1$. Dato che i diagrammi commutano si ha che $\beta(m) = f_1(\alpha(n)) = \beta(f(n)) \Rightarrow m = f(n)$. Dato che $m \in Imf \Rightarrow m \in Kerg \Rightarrow p = g(m) = 0$;

γ **suriettiva:** Sia $p_1 \in P_1$, per la suriettività di g_1, $\exists m_1 \in M_1$ tale che $g_1(m_1) = p_1 \Rightarrow \exists! m \in M$ tale che $\beta(m) = m_1$. Adesso, poiché il diagramma commuta, $\gamma(g(m)) = g_1(\beta(m)) = p_1$ e dunque si ha la tesi poiché ho trovato un elemento $g(m)$ la cui immagine è p_1 tramite γ.

⋈

2.2 Moduli su PID

In questa sezione vogliamo dare dei risultati per moduli su anelli che sono domini a ideali principali. Abbiamo visto come la struttura di un modulo sia, in un certo senso, simile a quella di uno spazio vettoriale, ma, come già osservato, non valgono le stesse proprietà. Negli spazi vettoriali finiti, ad esempio, vale la proprietà che se V è uno spazio vettoriale, $dimV = n$, e W è sottospazio di V, allora $dimW \leq n$. In generale questa proprietà non vale per i moduli liberi: prendiamo ad esempio $M = \mathbb{K}[x, y]$ come modulo su stesso; allora $N = (x, y)$ è un sottomodulo di M, ma non è libero e quindi non ha un rango. Vorremmo trovare delle condizioni sufficienti per far si che le proprietà degli spazi vettoriali si "trasferiscano" ai moduli. Vediamo che se prendiamo un A-modulo M con A PID si possono ottenere dei buoni risultati. Partiamo con questo:

Teorema 2.2.1 *Sia M un modulo libero su un PID A e sia $0 \neq N \subseteq M$ un sottomodulo, allora N è libero e $rkN \leq rkM$.*

Dimostrazione: Consideriamo solamente il caso finito (il caso infinito non è trattato). Svolgiamo la dimostrazione per induzione su $r = rkM$:
P. base: $r = 1$) Dato che $r = 1$ allora M è un modulo ciclico cioè $M \cong < m > \cong A$. Dato che A è PID e N è un sottomodulo di A, allora $N = (a)$ con $a \neq 0$ ideale principale. Dunque N è libero perché $\{a\}$ è un insieme di generatori linearmente indipendenti ($ka = 0 \Rightarrow k = 0$ perché A

è dominio);
P. induttivo: $r \Rightarrow (r+1)$) Sia $rkM = r+1$ e sia $\mathcal{B} = \{m_1, ..., m_r, m_{r+1}\}$ una base di M. Sia $0 \neq N \subseteq M$ sottomodulo e consideriamo $N_r = N \cap < m_1, ..., m_r >$. Adesso $< m_1, ..., m_r >$ è un modulo libero di rango r e N_r un suo sottomodulo; per ipotesi induttiva N_r è libero e $rkN_r \leq r$. Se $N = N_r$ ho la tesi, altrimenti vale che $N_r \subsetneq N$ e dunque $\exists n \in N$ tale che $n = b_1m_1 + ... + b_rm_r + a_nm_{r+1}$ con $a_n \neq 0$. Consideriamo

$$I = \{\alpha \in A | \ \exists n \in N \text{ t.c. } n = b_1m_1 + ... + b_rm_r + \alpha m_{r+1}\}$$

Come già osservato I è non vuoto, inoltre si verifica facilmente che I è un ideale di A, pertanto, dato che A è un PID, $I = (d)$. Dato che $d \in I \Rightarrow \exists n_d \in N$ tale che $n_d = c_1m_1 + ... + c_rm_r + dm_{r+1}$. Vogliamo dimostrare che $N = N_r \oplus < n_d >$ ottenendo la tesi poiché somma diretta di moduli liberi è libera. Costruiamo la successione:

$$0 \longrightarrow N_r \cap < n_d > \xrightarrow{f} N_r \oplus < n_d > \xrightarrow{g} N_r + < n_d > \longrightarrow 0$$

definita come nel lemma 2.1.19. Dato che la successione è esatta vale in particolare che $N_r + < n_d > \cong (N_r \oplus < n_d >)/Kerg \cong (N_r \oplus < n_d >)/Imf$; pertanto, dimostrando che $N_r + < n_d > = N$ e che $N_r \cap < n_d > = 0$ si ha la tesi:

$N_r + < n_d > = N$) Per costruzione vale che $N_r + < n_d > \subseteq N$. Viceversa sia $n \in N \Rightarrow n = b_1m_1 + ... + b_rm_r + a_nm_{r+1}$; $a_n \in I = (d) \Rightarrow \exists k \in A$ tale che $a_n = kd$. Allora $n = (n - kn_d) + kn_d$ dove il primo termine appartiene a N_r, il secondo a $< n_d >$;

$N_r \cap < n_d > = 0$) Sia $n \in N_r \cap < n_d > \Rightarrow n = b_1m_1 + ... + b_rm_r$ e $n = kc_1m_1 + ... + kc_rm_r + kdm_{r+1}$. Sottraendo membro a membro si ottiene $(b_1 - kc_1)m_1 + ... + (b_r - kc_r)m_r - kdm_{r+1} = 0$ e dato che $\{m_1, ..., m_{r+1}\}$ sono una base, $kd = 0$. Visto che A è dominio $k = 0$ e di conseguenza $b_1 = ... = b_r = 0$ cioè $N_r \cap < n_d > = 0$.

⋈

Proposizione 2.2.2 *Sia M modulo su un PID A, se M è finitamente generato e N è sottomodulo di M, allora N è finitamente generato.*

Dimostrazione: Come già osservato, se M è generato da r elementi allora $M \cong A^r/Kerf$ con $f : A^r \to M$ suriettiva. Consideriamo adesso $N_1 = f^{-1}(N)$; N_1 è sottomodulo di un modulo libero ed è pertanto libero per il teorema precedente. $N_1 =< n_1, ..., n_s >$ e dunque $f(N_1) = N$ è generato da $\{f(n_1), ..., f(n_s)\}$.

⋈

Definizione 2.20 *Una matrice $X \in M_n(A)$ con A anello si dice **invertibile** se $det(X) \in A^*$.*

Se $S \in M_n(A)$ è una matrice invertibile, allora questa può essere scritta come composizione di matrici elementari di Gauss, dove una matrice elementare di Gauss è ottenuta partendo dalla matrice identità e facendo una delle seguenti operazioni elementari:

1. Scambio di due righe;
2. Sommare a una riga un multiplo di un'altra riga;
3. Moltiplicare una riga per un elemento invertibile.

Definizione 2.21 *Due matrici $X, Y \in M(r \times s, A)$ si dicono **equivalenti** se esistono $S \in M_r(A)$, $T \in M_s(A)$ invertibili tali che $SXT = Y$.*

Lemma 2.2.3 *Sia $X \in M_2(A)$ con A dominio a ideali principali, allora esistono due matrici $S, R \in M_2(A)$ invertibili tali che $SX = T_s$ triangolare superiore e $XR = T_i$ triangolare inferiore.*

Dimostrazione: Sia $X \in M_2(A)$:

$$X = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

e consideriamo $x = MCD(a, b)$ e $y = MCD(a, c)$ che esistono poiché siamo in un PID. Dunque esistono $s, t, v, w \in A$ tali che $as + bt = x$ e $aw + cv = y$. Siano dunque $S, R \in M_2(A)$ invertibili, allora:

$$S = \begin{bmatrix} s & t \\ -\frac{b}{x} & \frac{a}{x} \end{bmatrix} \implies SX = \begin{bmatrix} x & m \\ 0 & n \end{bmatrix} = T_s$$

$$R = \begin{bmatrix} w & -\frac{c}{y} \\ v & \frac{a}{y} \end{bmatrix} \implies XR = \begin{bmatrix} y & 0 \\ l & k \end{bmatrix} = T_i$$

⋈

Osservazione: Grazie al lemma precedente è possibile rendere triangolare superiore o inferiore la matrice di testa 2×2 di una matrice qualsiasi di dimensioni $r \times s$: rimanendo nelle notazioni precedenti, basta infatti moltiplicare a blocchi per le matrici:

$$S = \begin{bmatrix} s & t & & \\ -\frac{b}{x} & \frac{a}{x} & & \\ & & & \\ & & I_{r-2} & \end{bmatrix} \qquad R = \begin{bmatrix} w & -\frac{c}{y} & & \\ v & \frac{a}{y} & & \\ & & & \\ & & & I_{s-2} \end{bmatrix}$$

Lemma 2.2.4 *Sia A un PID e $X \in M(r \times s, A)$ una matrice, allora esistono due matrici $S \in M_r(A), R \in M_s(A)$ invertibili tali che SXR è nella forma:*

$$\begin{bmatrix} x & 0 & ... & 0 \\ 0 & & & \\ \vdots & & X_1 & \\ 0 & & & \end{bmatrix}$$

Dimostrazione: Sia $X_0 = X \in M(r \times s, A)$:

$$X_0 = \begin{bmatrix} x_0 & a_{0,2} & a_{0,3} & ... & a_{0,s} \\ b_{0,2} & c_0 & & & \\ \vdots & & & \overline{X_0} & \\ b_{0,r} & & & & \end{bmatrix}$$

Applichiamo adesso il seguente algoritmo:

```
Input: X
Finché in posizione (1,1) non compare il solito termine per r+s cicli ripeti:
    for i=2:r
        scambia la riga 2 con la riga i;
        rendi triangolare superiore la matrice di testa 2 x 2;
    endfor
```

```
    for i=2:s
        scambia la colonna 2 con la colonna i;
        rendi triangolare inferiore la matrice di testa 2 x 2;
    endfor
endwhile
Output: X_N
```

L'algoritmo descritto crea una successione di matrici della forma:

$$\begin{bmatrix} x_0 & a_{0,2} & \dots & a_{0,s} \\ b_{0,2} & c_0 & & \\ \vdots & & \overline{X_0} & \\ b_{0,r} & & & \end{bmatrix} \longrightarrow \begin{bmatrix} x_1 & a_{1,2} & \dots & a_{1,s} \\ 0 & c_1 & & \\ \vdots & & \overline{X_1} & \\ b_{1,r} & & & \end{bmatrix} \longrightarrow \dots \longrightarrow \begin{bmatrix} x_n & 0 & \dots & a_{n,s} \\ b_{n,2} & c_n & & \\ \vdots & & \overline{X_n} & \\ b_{n,r} & & & \end{bmatrix} \longrightarrow \dots$$

e, per costruzione, vale la seguente relazione: $x_{i+1}|x_i$. Si viene dunque a formare una successione di ideali

$$(x_0) \subseteq (x_1) \subseteq (x_2) \subseteq \dots \subseteq (x_n) \subseteq \dots$$

Consideriamo adesso $I = \bigcup_i (x_i)$; si dimostra facilmente che I è un ideale di A e pertanto $I = (c)$, ma allora esisterà un $N \in \mathbb{N}$ tale che $c \in (x_N)$ e dunque la catena si stabilizza dopo l'ideale (x_N). Consideriamo allora

$$X_N = \begin{bmatrix} x_N & 0 & \dots & a_{N,s} \\ b_{N,2} & c_N & & \\ \vdots & & \overline{X_N} & \\ b_{N,r} & & & \end{bmatrix}$$

Dato che la catena si stabilizza, l'algoritmo termina e, al passo N-esimo si ha che x_N e $x_{N+1} = MCD(b_{N,2}, x_N)$ sono associati e quindi $x_N|b_{N,2} \Rightarrow b_{N,2} = dx_N$. A questo punto, invece di applicare la solita operazione elementare descritta nell'algoritmo, togliamo alla seconda riga la prima riga moltiplicata per d. Iteriamo il procedimento di annullamento per tutti gli altri termini della prima riga e della prima colonna ottenendo la tesi.

⋈

Definizione 2.22 *Sia A un PID e $D \in M(r \times s, A)$ matrice diagonale $[D]_{i,j} = d_i$ se $i = j$, 0 altrimenti; D si dice in* ***forma normale di Smith*** *se $d_i|d_{i+1}$ per ogni $i = 1, 2..., min(r, s) - 1$.*

Lemma 2.2.5 *Sia A un PID e $D \in M(r \times s, A)$ matrice diagonale con $[D]_{i,i} = d_i$, allora, mediante operazioni elementari di riga e di colonna è possibile portare D in forma normale di Smith.*

Dimostrazione: Se la matrice diagonale è in forma normale di Smith ho finito, altrimenti esiste i indice minimo tale che d_i non divide d_{i+1}. Detto allora $x = MCD(d_i, d_{i+1})$ e dunque $t, s \in A$ tali che $sd_i + td_{i+1} = x$ moltiplico D a sinistra per $S \in M_r(A)$ e a destra per $R \in M_s(A)$ invertibili così definite:

$$S = \begin{bmatrix} I_{i-1} & & & \\ & s & t & \\ & -\frac{d_{i+1}}{x} & \frac{d_i}{x} & \\ & & & I_{r-i-1} \end{bmatrix} \qquad R = \begin{bmatrix} I_{i-1} & & & \\ & 1 & -\frac{-td_{i+1}}{x} & \\ & 1 & \frac{sd_i}{x} & \\ & & & I_{s-i-1} \end{bmatrix}$$

Con facili conti si ottiene la seguente matrice:

$$SXR = \begin{bmatrix} D_{i-1} & & & \\ & x & 0 & \\ & 0 & \frac{d_i d_{i+1}}{x} & \\ & & & \tilde{D} \end{bmatrix}$$

Iterando l'algoritmo, questo ha termine in un numero finito di passi (grazie al fatto che la matrice ha dimensione finita) e porta la matrice D in forma normale di Smith mediante operazioni elementari.

⋈

Teorema 2.2.6 (Forma normale di Smith) *Sia A un dominio a ideali principali e sia $X \in M(r \times s, A)$, allora X è equivalente a una matrice diagonale D in forma normale di Smith.*

Dimostrazione: Applicando i lemmi dimostrati, si porta in forma diagonale la matrice X (si azzerano la prima riga e la prima colonna e poi si considera la matrice $(r-1) \times (s-1)$ e si fa la stessa cosa), e poi si porta la forma diagonale in forma di Smith.

⋈

Proposizione 2.2.7 *Sia A un PID e $X \in M(r \times s, A)$, detto $\Delta_i(X)$ l'ideale generato dai determinanti di tutte le sottomatrici $i \times i$ di X, $\Delta_i = (\delta_i)$ allora, se X è equivalente a Y, $\Delta_i(X) = \Delta_i(Y)$ per ogni i. Sia inoltre D una forma normale di Smith di X, vale allora la seguente relazione: $d_i = \frac{\delta_i}{\delta_{i-1}}$ e dunque la forma normale di Smith è unica.*

Dimostrazione: Mostriamo la prima parte dell'enunciato: siano $S \in M_r(A), R \in M_s(A)$ invertibili tali che $SXR = Y$. Consideriamo $X \to SX$: la matrice ottenuta ha come righe una combinazione lineare delle righe di X e pertanto i suoi determinanti $i \times i$ (grazie alla multilinearità del determinante) sono contenuti nell'ideale $\Delta_i(X)$; vale pertanto che $\Delta_i(SX) \subseteq \Delta_i(X)$. Inoltre, dato che S è invertibile, si ha che $\Delta_i(X) = \Delta_i(S^{-1}SX) \subseteq \Delta_i(SX)$ per lo stesso motivo. Ragionando in maniera analoga per le colonne di X si ottiene $\Delta_i(X) = \Delta_i(SXR) = \Delta_i(Y)$
Per quanto dimostrato, si ha che X è equivalente a D in forma di Smith con $d_1|d_2|...|d_n$ e pertanto $\Delta_1(X) = \Delta_1(D) = (d_1, ..., d_n) = (d_1) = (\delta_1)$. Inoltre $\Delta_2(X) = \Delta_2(D) = (d_1d_2, d_1d_3, ..., d_{n-1}d_n) = (d_1d_2) = (\delta_2)$. Iterando il procedimento si ha in generale $\Delta_i(X) = (d_1 \cdots d_i) = (\delta_i)$ e dunque la relazione (a meno di invertibili) $d_i = \frac{\delta_i}{\delta_{i-1}} = \frac{\Delta_i(X)}{\Delta_{i-1}(X)}$. Dato che i d_i dipendono in modo univoco da X la forma di Smith è unica.

⋈

Definizione 2.23 *Sia M A-modulo, A anello, si definisce **torsione di M** l'insieme*

$$T(M) = \{m \in M | \ \exists a \in A, a \neq 0 \text{ tale che } am = 0\}$$

*Se A è un dominio, allora l'insieme di torsione è sottomodulo di M e prende il nome di **sottomodulo di torsione di** M.*

Osservazione: Se A non è un dominio non è detto che l'insieme $T(M)$ sia un sottomodulo. Considriamo $\mathbb{Z}_6$ come modulo su se stesso. $T(\mathbb{Z}_6) = \{0, 2, 3, 4\}$ non è un sottomodulo poiché, ad esempio, non è chiuso per somma.

Lemma 2.2.8 *Sia N A-modulo e $N \cong A/J_1 \oplus A/J_2$ con J_1, J_2 ideali di A, se $I \subseteq A$ ideale allora $N/IN \cong A/(J_1 + I) \oplus A/(J_2 + I)$.*

Dimostrazione: $IN \cong I/(I \cap J_1) \oplus I/(I \cap J_2) \cong (I + J_1)/J_1 \oplus (I + J_2)/J_2$. Per il secondo teorema di omomorfismo, quozientando componente per componente si ha la tesi.

⋈

Lemma 2.2.9 *Sia $N = A/J$ A-modulo con J ideale di A, sia $a \in A$, allora $aN = A/(J : a)$.*

Dimostrazione: Consideriamo la mappa F

$$\begin{aligned} A &\longrightarrow A/J \longrightarrow aA/J \\ b &\longrightarrow b+J \longrightarrow a(b+J) \end{aligned}$$

La mappa $F : A \to aN$ è suriettiva perché composizione di funzioni suriettive. Cerchiamo $KerF$: $F(b) = 0 \Leftrightarrow a(b+J) = 0 \Longrightarrow ab \in J \Leftrightarrow b \in (J : a)$. Per il primo teorema di omomorfismo segue la tesi.

$\bowtie$

Lemma 2.2.10 *Sia B A-modulo e $m, n \in \mathbb{N}, m > n$, se esiste $\varphi : B^n \to B^m$ suriettiva, allora $B = 0$.*

Dimostrazione: Supponiamo, $B \neq 0$; consideriamo

$$B^m = B^n \oplus B^{m-n} \xrightarrow{\pi} B^n \xrightarrow{\varphi} B^m$$

La composizione $F = \varphi \circ \pi$ è suriettiva e pertanto è un endomorfismo suriettivo e dunque, per Nakayama, è iniettivo. Pertanto π deve essere iniettiva, ma questo è assurdo poiché, ad esempio, $\pi(e_m) = 0$.

$\bowtie$

NOTA DI RICHIAMO: Per poter dimostrare i risultati successivi abbiamo bisogno di introdurre una notazione matriciale per esprimere un morfismo $f : A^r \to A^s$. In particolare siano $\mathcal{B}_1 = \{\alpha_1, ..., \alpha_r\}$ base di A^r e $\mathcal{B}_2 = \{\beta_1, ..., \beta_s\}$ base di A^s. Il morfismo f è completamente determinato da dove viene mandata $\mathcal{B}_1$ e inoltre possiamo identificare le immagini degli elementi di $\mathcal{B}_1$ tramite f con le loro coordinate rispetto alla base $\mathcal{B}_2$. Grazie a questa idea (che è la stessa che utilizziamo con gli spazi vettoriali) possiamo portare f in forma matriciale rispetto alle basi $\mathcal{B}_1$ e $\mathcal{B}_2$ nel seguente modo:

$$\mathcal{M}_{\mathcal{B}_1,\mathcal{B}_2}(f) = \big([f(\alpha_1)]_{\mathcal{B}_2} \quad | \quad [f(\alpha_2)]_{\mathcal{B}_2} \quad | \quad ... \quad | \quad ... \quad | \quad [f(\alpha_r)]_{\mathcal{B}_2}\big)$$

con $\mathcal{M}_{\mathcal{B}_1,\mathcal{B}_2}(f)$ matrice $s \times r$. Ogni morfismo tra due A-moduli liberi si può dunque vedere come una matrice.

Teorema 2.2.11 *Se M è un modulo finitamente generato su un dominio a ideali principali A, allora M si scrive in modo unico come $M \cong A^k \oplus T(M)$.*

Dimostrazione: Supponiamo che M sia generato dall'insieme $\{m_1, ..., m_r\}$. Come abbiamo osservato possiamo vedere M come quoziente tra A^r con base $\mathcal{B}_r = \{\alpha_1, ..., \alpha_r\}$ e il Ker del morfismo suriettivo $f : A^r \to M$, $f(e_i) = m_i$. Possiamo pertanto creare la seguente successione esatta corta:

$$0 \longrightarrow Kerf \longrightarrow A^r \xrightarrow{f} M \longrightarrow 0$$

$Kerf$ è sottomodulo di un modulo libero su PID e pertanto è anch'esso libero. Sia dunque $\mathcal{B} = \{w_1, ..., w_s\}$ una base di $Kerf$ e sia $\mathcal{B}_s = \{\eta_1, ..., \eta_s\}$ una base di A^s. Costruiamo la successione:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Kerf & \longrightarrow & A^r & \xrightarrow{f} & M & \longrightarrow & 0 \\ & & \varphi \big\downarrow & \nearrow_{g} & & & & & \\ 0 & \longrightarrow & A^s & & & & & & \end{array}$$

Con φ isomorfismo tale che $\varphi(w_i) = \eta_i$ per ogni i. Per l'esattezza delle successioni si ha che $M \cong A^r/Kerf \cong A^r/Img \cong CoKerg$. Per quanto osservato, fissate le basi $\mathcal{B}_s, \mathcal{B}_r$, possiamo vedere il morfismo $g : A^s \to A^r$ come una matrice $X \in M(r \times s, A)$. Grazie ai teoremi precedenti, possiamo scegliere due basi $\mathcal{D}_s = \{\gamma_1, ..., \gamma_s\}, \mathcal{D}_r = \{\beta_1, ..., \beta_r\}$ tali che $\mathcal{M}_{\mathcal{D}_s,\mathcal{D}_r}(g) = D$ è in forma di Smith con $d_1|d_2|...|d_s$, e valgono le seguenti relazioni: $X[v]_{\mathcal{B}_s} = [g(v)]_{\mathcal{B}_r}$ e $D[v]_{\mathcal{D}_s} = [g(v)]_{\mathcal{D}_r}$ e $g(\gamma_i) = d_i\beta_i = (0, ..., 0, d_i, 0, ..., 0)$. Pertanto, quozientando componente per componente,

$$M \cong CoKerg \cong A/(d_1) \oplus ... \oplus A/(d_s) \cong \bigoplus_{i=1}^{s} A/(d_i)$$

con $(d_1) \supseteq (d_2) \supseteq ... \supseteq (d_s)$. Dobbiamo verificare che la scelta dei generatori iniziali di M non influisce sull'unicità della scrittura. Supponiamo quindi

$$M \cong \bigoplus_{i=1}^{n} A/(I_i) \cong \bigoplus_{i=i}^{m} A/(J_i)$$

con $I_1 \supseteq ... \supseteq I_n$ e $J_1 \supseteq ... \supseteq J_m$ con $m > n$, vogliamo dimostrare che $J_1 = ... = J_{m-n} = A$ e $J_{m-n+i} = I_i$ per $i = 1, ..., n$. Sia $B = A/J_1$ e consideriamo

$$B^m \cong \bigoplus_{i=1}^{m} A/J_1 \cong \bigoplus_{i=1}^{m} A/(J_1 + J_i) \cong M/J_1M \cong \bigoplus_{i=1}^{n} A/(J_1 + I_i)$$

dove la prima uguaglianza deriva dal fatto che $J_i \subseteq J_1$ per ogni i e le ultime derivano dal lemma 2.2.9. Esiste dunque la proiezione al quoziente $\pi : B^n \to \bigoplus_{i=1}^{n} A/(J_1 + I_i) = B^m$; essendo questa suriettiva, per il lemma 2.2.10, $B = 0 \Rightarrow A = J_1$. Iterando il procedimento per ogni $i = 1, ..., m - n$, $J_i = A$. Possiamo quindi supporre $m = n$, vogliamo adesso mostrare che $J_i = I_i$ per ogni $i = 1, ..., n$. Ci basta far vedere una inclusione, l'altra si ottiene per simmetria: sia $a \in I_i$ e consideriamo

$$\bigoplus_{i=1}^{n} A/(I_i : a) \cong a\bigoplus_{i=1}^{n} A/I_i \cong aM \cong a\bigoplus_{i=1}^{n} A/J_i \cong \bigoplus_{i=1}^{n} A/(J_i : a)$$

Adesso $(I_j : a) = A$ per $j = 1, ..., i$ e dunque

$$\bigoplus_{j=i+1}^{n} A/(I_j : a) \cong \bigoplus_{j=1}^{n} A/(J_j : a)$$

con $(J_1 : a) \supseteq ... \supseteq (J_n : a)$. Ricalcando quanto dimostrato in precedenza si deve avere che $(J_j : a) = A$ per ogni $j = 1, ..., i$, cioè, in particolare, $a \in J_i$. Abbiamo dunque dimostrato l'unicità della scrittura:

$$M \cong A/(d_1) \oplus ... \oplus A/(d_s) \cong T(M) \oplus A^{s-n}$$

con $T(M) \cong A/(d_1) \oplus ... \oplus A/(d_n)$ e $(d_{n+1}) = ... = (d_s) = 0$

⋈

Definizione 2.24 *Sia M A-modulo con A dominio, definiamo la* ***d-esima componente di M*** *l'insieme:*

$$M_d = \{m \in M |\ \exists k \in \mathbb{N} \text{ tale che } d^k m = 0\}$$

Se inoltre d è primo e $M = M_d$ allora M si dice ***d-primario****.*

Proposizione 2.2.12 *Sia M A-modulo p-primario finitamente generato con A PID, allora*

$$M \cong A/(p^{k_1}) \oplus ... \oplus A/(p^{k_s})$$

con $k_1 \leq k_2 \leq ... \leq k_s$.

Dimostrazione: Per il teorema precedente $M \cong T(M) \oplus A^k \cong A/(d_1) \oplus ... \oplus A/(d_s) \oplus A^k$ per certi $k, s \in \mathbb{N}$. Dato che M è p-primario, $M \cong T(M)$: supponiamo per assurdo che esista parte libera, e che $p^k(\bar{m_1}, ..., \bar{m_s}, m_{s+1}, ..., m_k) = 0 \Rightarrow \forall i = s+1, ..., k$ si ha che $p^k m_i = 0$, ma dato che la relazione vale in $A \Rightarrow m_i = 0$ e dunque la parte libera è banale. Dimostriamo adesso che $p|d_i$ per ogni $i = 1, ..., s$: come prima $p^k(\bar{m_1}, ..., \bar{m_s}) = 0 \Rightarrow p^k \bar{m_i} = \bar{0} \Rightarrow p^k m_i \in (d_i) \Rightarrow p^k m_i = d_i t_1$. Supponiamo che $m_i \notin (d_i)$. p divide il membro di sinistra ed è primo, pertanto $p|d_i$ o $p|t_1$; nel primo caso si ha la tesi, altrimenti, se $p|t_1 \Rightarrow t_1 = pt_2$ e si ha la relazione $p^{k-1} m_1 = d_i t_2$. Iterando il procedimento supponendo che p divida t_j ad ogni passo si ottiene $m_i = d_i t_k$ cioè $m_i \in (d_i)$, contro l'ipotesi. Pertanto $p|d_i$ per ogni $i = 1, ..., s$. Consideriamo adesso la s-upla $(\bar{1}, ..., \bar{1}) \in M$; per ipotesi $p^k(\bar{1}, ..., \bar{1}) = 0$ e pertanto, componente per componente, $p^k \in (d_i) \Rightarrow d_i | p^k$. Allora per ogni i, $p|d_i|p^k \Rightarrow d_i = p^n$ con $n < k$.

⋈

Proposizione 2.2.13 *Sia M A-modulo finitamente generato, allora*

$$M \cong A^k \bigoplus \Big(\bigoplus_{i=1}^{h} A/(q_i) \Big)$$

con (q_i) ideali primari di A.

Dimostrazione: Per il teorema precedente $M \cong T(M) \oplus A^k \cong A/(d_1) \oplus ... \oplus A/(d_s) \oplus A^k$ con $d_i = p_{i,1}^{t_{i,1}} \cdots p_{i,r}^{t_{i,r}}$. Per il teorema cinese del resto

$$A/(d_i) = A/(p_{i,1}^{t_{i,1}}) \oplus ... \oplus A/(p_{i,r}^{t_{i,r}})$$

e $(p_{i,j}^{t_{i,j}})$ è ideale primario di A per ogni i, j.

⋈

ESERCIZIO: Sia $M = A^k \oplus T(M)$ un A-modulo, A dominio, dimostrare che:

1. $M/T(M)$ è libero da torsioni;
2. Dati N e P A-moduli e la successione esatta corta $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$, esistono $\bar{f}$ e $\bar{g}$ tali che la successione $0 \to T(M) \xrightarrow{\bar{f}} T(N) \xrightarrow{\bar{g}} T(P)$ è esatta a sinistra

Soluzione:

1. Consideriamo un $\bar{m} \in T(M/T(M))$ allora $\exists a \in A, a \neq 0$ t.c $a(m + T(M)) = 0$ ovvero $am \in T(M) \Rightarrow \exists b \in A, b \neq 0$ t.c $bam = 0$ dunque $\bar{m} = \bar{0}$;
2. Mostriamo intanto che se $h : B \to C$ è un omomorfismo di A-moduli, allora $h(T(B)) \subseteq T(C)$: sia $b \in T(B)$ allora $\exists a \in A$ tale che $ab = 0$, visto che h è A-lineare si ha $0 = h(ab) = ah(b) \Rightarrow h(b) \in T(C)$. Abbiamo dunque la successione $0 \to T(M) \xrightarrow{\bar{f}} T(N) \xrightarrow{\bar{g}} T(P)$, dove $\bar{f} = f_{|T(M)}$ e $\bar{g} = g_{|T(N)}$. Ora $\bar{f}$ è iniettiva in qualità di restrizione di una funzione iniettiva, dunque, per l'esattezza della successione, resta da far vedere che $Ker\bar{g} = Im\bar{f}$. Mostriamo le due inclusioni :
   $\subseteq$) Sia $n \in Ker\bar{g} \subseteq T(N)$ allora $\bar{g}(n) = g(n) = 0 \Rightarrow n \in Ker(g) = Im(f)$, esiste quindi un

certo $m \in M$ tale che $f(m) = n$. Vale in realtà $m \in T(M)$: il fatto che n appartenga in particolare a $T(N)$ implica l'esistenza di $d \in A$ non nullo tale che $dn = 0 = df(m) = f(dm)$, per l'iniettività di f, abbiamo $dm = 0$ e $m \in T(M)$, quindi $n \in Im\bar{f}$.
$\supseteq$) Se $m \in T(M)$, grazie all'esattezza della successione di partenza, abbiamo $\bar{g}(\bar{f}(m)) = g(f(m)) = 0 \Rightarrow Ker\bar{g} \supseteq Im\bar{f}$.

Definizione 2.25 *Un A-modulo M non nullo si dice* ***semplice*** *se non ha sottomoduli non banali*

ESERCIZIO: Si dimostrino i seguenti fatti

1. Dato M un A-modulo vale: M è semplice $\Leftrightarrow M \neq 0$ e $\forall m \in M$, $m \neq 0$, $< m >= M$;

2. Gli $\mathbb{Z}$-moduli semplici sono tutti e soli quelli della forma $\mathbb{Z}_p$, p primo;

3. Se $\varphi_{a,b} : \mathbb{Z}_3 \to M$ è un omomorfismo di $\mathbb{Z}$-moduli surgettivo tale che $Ker\varphi =< m_1, m_2, m_3 >$ con $m_1 = (2, 4, 6)$, $m_2 = (0, a, 2a)$, $m_3 = (b, 4, 6)$, e $a, b \in \mathbb{Z}$, allora esistono $a, b \in \mathbb{Z}$ tali che M è semplice.

Soluzione:

1. $\Rightarrow$) Se il sottomodulo $< m >$ è non nullo allora, per la semplicità di M, si deve avere $< m >= M$.
$\Leftarrow$) Sia $N \subseteq M$ un sottomodulo non nullo e $n \in N$, $n \neq 0$, allora $< n >\subseteq N \subseteq M \Rightarrow <$ $n >= M \Rightarrow N = M$;

2. Cerchiamo $\mathbb{Z}$-moduli ciclici e, grazie al punto uno, tali che ogni elemento generi tutto il modulo. Gli $\mathbb{Z}$-moduli sono i gruppi abeliani, e pertanto cerchiamo tra gli $\mathbb{Z}_n$ i moduli semplici. La condizione che ogni elemento diverso da 0 generi il modulo ci dice che ogni elemento deve avere ordine additivo esattamente n e questa è una proprietà che hanno soltanto gli $\mathbb{Z}_p$ con p primo;

3. Usiamo la forma di Smith:

$$\begin{array}{ccccc} \mathbb{Z}_3 & \xrightarrow{f} & \mathbb{Z}_3 & \xrightarrow{\varphi_{a,b}} & M \\ e_i & \longrightarrow & m_i & & \end{array}$$

$M \cong \mathbb{Z}_3/Ker\varphi_{a,b} \cong CoKerf$, studiamo il $CoKerf$:

$$\begin{bmatrix} 2 & 0 & b \\ 4 & a & 4 \\ 6 & 2a & 6 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 0 & b \\ 0 & a & 4-2b \\ 0 & 2a & 4-3b \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 0 & b \\ 0 & a & 4-2b \\ 0 & 0 & b-2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b-2 \end{bmatrix}$$

Abbiamo quindi $\Delta_1 = (MCD(2, a, b-2)) = (\delta_1)$, $\Delta_2 = (MCD(2a, 2(b-2), a(b-2))) = (MCD(a, b-2)) = (\delta_2)$, $\Delta_3 = (2a(b-2)) = (\delta_3)$. Affinché M sia uno $\mathbb{Z}_p$ mi occorre $d_1 = d_2 = 1$ e $d_3 = p$, p primo, con d_1, d_2, d_3 elementi diagonali della forma di Smith. Ricordando che $d_1 = \delta_1$, $d_2 = \delta_2/\delta_1$, e $d_3 = \delta_3/\delta_2 = 2a(b-2)/MCD(a, b-2)$, le condizioni sono soddisfatte per le coppie $\{(1, 3), (1, 1), (-1, 3), (-1, 1)\}$.

2.3 Successioni e moduli proiettivi

Diamo qualche definizione preliminare di teoria delle categorie per poter capire meglio i prossimi argomenti. In particolare introduciamo il concetto di categoria $\mathcal{C} = (Obj(\mathcal{C}), Mor(\mathcal{C})$ dove $Obj(\mathcal{C})$ sono gli oggetti di una categoria e $Mor(\mathcal{C})$ sono la mappe tra una coppia di oggetti appartenenti alla categoria. La categoria è inoltre dotata dell'intuitiva legge di composizione tra i morfismi; soddisfa inoltre i seguenti due assiomi:

A1. Associatività della composizione;

A2. $\forall A \in Obj(\mathcal{C})\ \exists f \in Mor(\mathcal{C})$, $f : A \to A$ tale che $\forall h, g \in Mor(\mathcal{C})$ con $g : A \to B$ e $h : D \to A$ con $B, D \in Obj(\mathcal{C})$, si ha $f \circ h = h$ e $g \circ f = g$. Denoteremo f con id_A.

Diamo alcuni esempi di categorie:

1. $\mathcal{C} = Set$, $Obj(\mathcal{C})$ = insiemi, $Mor(\mathcal{C})$ = funzioni tra insiemi;
2. $\mathcal{C} = Ring$, $Obj(\mathcal{C})$ = anelli, $Mor(\mathcal{C})$ = omomorfismi tra anelli;
3. $\mathcal{C} = Top$, $Obj(\mathcal{C})$ = spazi topologici, $Mor(\mathcal{C})$ = funzioni continue tra spazi topologici;

Date due categorie $\mathcal{C}, \mathcal{D}$, vorremmo metterle in relazione, confrontando sia gli oggetti che i morfismi; a tale scopo introduciamo il concetto di funtore:

Definizione 2.26 *Siano $\mathcal{C}, \mathcal{D}$ due categorie, definiamo una mappa $F : \mathcal{C} \to \mathcal{D}$ tale che $\forall A \in Obj(\mathcal{C})$, $F(A) \in Obj(\mathcal{D})$, $\forall f \in Mor(\mathcal{C})$ $F(f) \in Mor(\mathcal{D})$ e $F(id_A) = id_{F(A)}$. F è detto **funtore**. In particolare, se $f \in Mor(\mathcal{C})$, $f : A \to B$ allora deve valere una delle seguenti due condizioni:*

- *$F(f) : F(A) \to F(B)$ (**funtore covariante**). Se $g \in Mor(\mathcal{C})$, $g : B \to D$, $F(g \circ f) = F(g) \circ F(f)$;*
- *$F(f) : F(B) \to F(A)$ (**funtore controvariante**). Se $g \in Mor(\mathcal{C})$, $g : B \to D$, $F(g \circ f) = F(f) \circ F(g)$;*

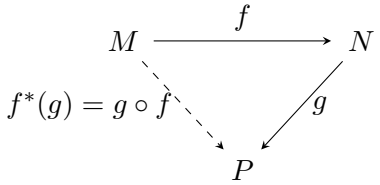
Facciamo alcuni esempi date $\mathcal{C}, \mathcal{D}$ categorie:

Funtore costante: Trasforma ogni oggetto di $\mathcal{C}$ in un oggetto $X \in Obj(\mathcal{D})$ fissato e ogni morfismo di $\mathcal{C}$ in id_X;

Funtore dimenticante: Si dimentica solamente della struttura degli oggetti della categoria di partenza. Ad esempio, se $\mathcal{C} = Ring$, $\mathcal{D} = Set$ allora $F(A)$ con $A \in \mathcal{C}$ non è più dotato di somma e prodotto e $F(f)$ con f morfismo di anelli diventa una semplice funzione.

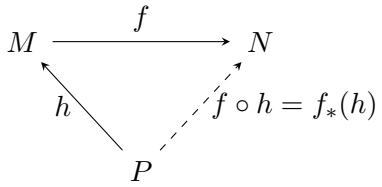
Definizione 2.27 *Un funtore si dice **esatto** se trasforma successioni esatte in successioni esatte.*

Definizione 2.28 *Siano M, N, P A-moduli, $f \in Hom(M, N)$, $\mathcal{C}(A)$ = categoria degli A-moduli, allora $\forall g \in Hom(N, P)$ consideriamo il grafico*



e definiamo il funtore $F = Hom(\star, P) : \mathcal{C}(A) \to \mathcal{C}(A)$ tale che $F(f) = Hom(\star, P)(f) = Hom(f, P) = f^*$ e $F(N) = Hom(\star, P)(N) = Hom(N, P)$ con $f^* : Hom(N, P) \longrightarrow Hom(M, P)$ tale che $f^*(g) = g \circ f$.

Definizione 2.29 *Siano M, N, P A-moduli, $f \in Hom(M,N)$, $\mathcal{C}(A)$ =categoria degli A-moduli, allora $\forall h \in Hom(P,M)$ consideriamo il grafico*



e definiamo il funtore $G = Hom(P,\star) : \mathcal{C}(A) \to \mathcal{C}(A)$ tale che $G(f) = Hom(P,\star)(f) = Hom(P,f) = f_*$ e $G(N) = Hom(P,\star)(N) = Hom(P,N)$ con $f_* : Hom(P,M) \longrightarrow Hom(P,N)$ tale che $f_*(h) = f \circ h$.

OSSERVAZIONE: notiamo quindi che il funtore $Hom(\star,P)$ è controvariante, e il funtore $Hom(P,\star)$ è covariante.

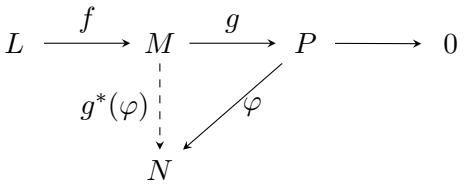
Teorema 2.3.1 *Siano L, M, P A-moduli, allora sono fatti equivalenti:*

1. *La successione $L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ è esatta;*
2. *$\forall N$ A-modulo la successione $0 \longrightarrow Hom(P,N) \xrightarrow{g^*} Hom(M,N) \xrightarrow{f^*} Hom(L,N)$ è esatta.*

Dimostrazione:

$1 \Rightarrow 2$) Per dimostrare che la successione è esatta dobbiamo mostrare che è esatta in ogni nodo:

g^* **iniettiva:** Vorremmo far vedere che se $\varphi \in Kerg^* \Rightarrow \varphi = 0$. Per fissare le idee costruiamo il grafico della situazione:

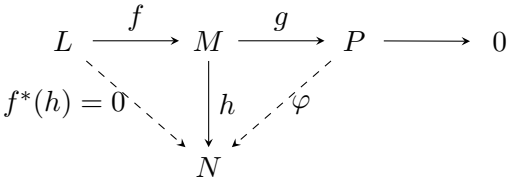


$g^*(\varphi) = 0 \Rightarrow \forall m \in M, (\varphi \circ g)(m) = \varphi(g(m)) = 0$. Per ipotesi g è suriettiva e pertanto $\forall p \in P$, $\exists m \in M$ tale che $g(m) = p$; ma allora $\varphi(g(m)) = \varphi(p) = 0$ $\forall p \in P \Rightarrow \varphi = 0$;

$Kerf^* = Img^*$**:** Dimostriamo i due contenimenti:

$\supseteq$) Sia $h \in Img^* \Rightarrow \exists \varphi$ tale che $h = g^*(\varphi) = \varphi \circ g$. Ora $f^*(h) = h \circ f = (\varphi \circ g) \circ f = \varphi \circ (g \circ f) = 0$ poiché $g \circ f = 0$ per l'ipotesi di esattezza della successione;

$\subseteq$) Sia $h \in Kerf^*$, vogliamo creare φ tale che $g^*(\varphi) = h$. La situazione è così schematizzata:

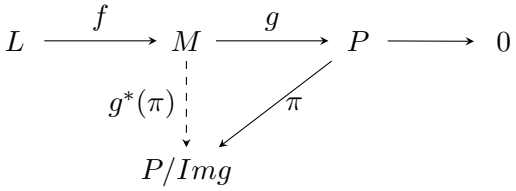


Per definire φ dobbiamo dire per ogni $p \in P$ chi è $\varphi(p)$. Dato che g è suriettiva, per ogni $p \in P$, $\exists m \in M$ tale che $g(m) = p$; definiamo dunque con queste

notazioni $\varphi(p) = h(m)$ e verifichiamo che φ è ben definita. Sia dunque m_1 tale che $g(m) = g(m_1) = p$, vogliamo mostrare che $h(m) = h(m_1)$ o, equivalentemente, che $h(m - m_1) = 0$. $g(m - m_1) = 0 \Rightarrow (m - m_1) \in Kerg = Imf$ per l'ipotesi di esattezza, ma allora $(m - m_1) = f(l)$ per un certo $l \in L$. Pertanto $h(m - m_1) = h(f(l)) = f^*(h)(l) = 0$ perché $h \in Kerf$. Visto che φ è ben definita e che $h = \varphi \circ g = g^*(\varphi)$ si ha la tesi;

$2 \Rightarrow 1$) Come sopra, per dimostrare che la successione è esatta, dobbiamo dimostrare che è esatta in ogni nodo. Per ipotesi, la successione $0 \longrightarrow Hom(P, N) \xrightarrow{g^*} Hom(M, N) \xrightarrow{f^*} Hom(L, N)$ è esatta per ogni N A-modulo e pertanto nella dimostrazione sceglieremo degli A-moduli adatti al nostro intento:

g **suriettiva:** Sia $N = P/Img$ e consideriamo la proiezione $\pi : P \to P/Img$; otteniamo:

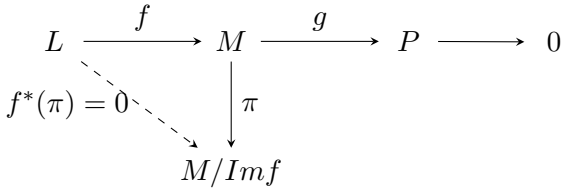


Vale che g è suriettiva $\Leftrightarrow P/Img = 0 \Leftrightarrow \pi = 0$. Per ogni $m \in M$, $g^*(\pi)(m) = (\pi \circ g)(m) = \pi(g(m)) = 0 \Rightarrow g^*(\pi) = 0$. Per ipotesi g^* è iniettiva e pertanto $\pi = 0$;

$Kerg = Imf$**:** Dimostriamo i due contenimenti:

$\supseteq$) Sia $N = P$ e $id : P \to P$. $m = f(l) \Rightarrow g(m) = g(f(l)) = f^*(g)(l) = f^*(g^*(id))(l) = ((f^* \circ g^*) \circ id)(l) = 0$ poiché $f^* \circ g^* = 0$ per ipotesi di esattezza della successione;

$\subseteq$) Sia $N = M/Imf$ e consideriamo la proiezione $\pi : M \to M/Imf$; otteniamo:



$f^*(\pi) = \pi \circ f = 0 \Rightarrow \pi \in Kerf^* = Img^* \Rightarrow \exists h \in Hom(P, N)$ tale che $g^*(h) = h \circ g = \pi$. Adesso $Kerg \subseteq Ker\pi = Imf \Rightarrow Kerg \subseteq Imf$.

⋈

Teorema 2.3.2 *Siano L, M, P A-moduli, allora sono fatti equivalenti:*

1. *La successione $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P$ è esatta;*
2. *$\forall N$ A-modulo la successione $0 \longrightarrow Hom(N, L) \xrightarrow{f_*} Hom(N, M) \xrightarrow{g_*} Hom(N, P)$ è esatta.*

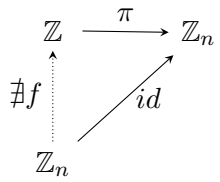
Dimostrazione: Svolgimento analogo al precedente.

⋈

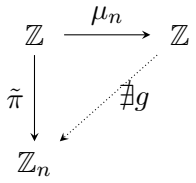
Il teorema mostra l'esattezza a sinistra della successione degli omomorfismi, in generale infatti la successione NON è esatta anche a destra.

Esempio: Data la successione $0 \to \mathbb{Z} \xrightarrow{\mu_n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \to 0$ esatta, con $\mu_n(m) = nm \ \forall m \in \mathbb{Z}$, scegliamo, nelle notazioni precedenti, $N = \mathbb{Z}_n$. La successione $0 \to Hom(\mathbb{Z}_n, \mathbb{Z}) \xrightarrow{\mu_*} Hom(\mathbb{Z}_n, \mathbb{Z}) \xrightarrow{\pi_*}$

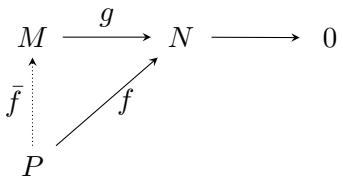
$Hom(\mathbb{Z}_n, \mathbb{Z}_n)$ non è esatta a destra: non esiste infatti una $f \in Hom(\mathbb{Z}_n, \mathbb{Z}) = 0$ t.c $\pi_*(f) = \pi \circ f = id_{\mathbb{Z}_n}$:



Ancora con $N = \mathbb{Z}_n$ si dimostra che nemmeno la successione $0 \to Hom(\mathbb{Z}_n, \mathbb{Z}_n) \xrightarrow{\pi^*} Hom(\mathbb{Z}, \mathbb{Z}_n) \xrightarrow{\mu_n^*} Hom(\mathbb{Z}, \mathbb{Z}_n)$ è esatta a destra: presa una generica $g \in Hom(\mathbb{Z}, \mathbb{Z}_n)$ t.c $g(1) = \bar{k}$ si ha $\mu_n^*(g)(1) = (g \circ \mu_n)(1) = g(n) = kn = \bar{0}$, quindi, per esibire un elemento che non appartiene all'immagine di μ_n^* basta prendere ad esempio la proiezione $\tilde{\pi} \in Hom(\mathbb{Z}, \mathbb{Z}_n)$:



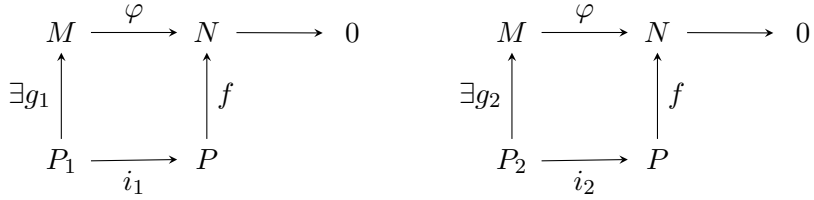
Definizione 2.30 *Siano P, M e N A-moduli. P si dice **proiettivo** se $\forall g \in Hom(M, N)$ surgettivo e $\forall f \in Hom(P, N)$ $\exists \bar{f} \in Hom(P, M)$ t.c. $g \circ \bar{f} = f$, ovvero la mappa f si solleva. In particolare il funtore $Hom(Q, \star)$ è esatto anche a destra.*



Osservazione: Un modulo libero è proiettivo: nelle notazioni precedenti, sia P libero e sia $\mathcal{B} = \{p_1, p_2, ..., p_n, ...\}$ una base di P, sia $f : P \to N$ un morfismo tale che $f(p_i) = n_i$ per tutti gli elementi della base (la condizione è sufficiente per definire il morfismo). Dato che g è suriettiva, $\forall n_i$ raggiunto da f esiste $m_i \in M$ tale che $g(m_i) = n_i$. A questo punto è sufficiente definire $\bar{f} : P \to M$ tale che $\bar{f}(p_i) = m_i$ per avere che P è proiettivo (infatti $g \circ \bar{f} = f$).

Proposizione 2.3.3 *Siano P, P_i A-moduli per ogni i, $P = \bigoplus_i P_i$. Allora P è proiettivo $\Leftrightarrow$ P_i è proiettivo $\forall i$.*

Dimostrazione: Ci limitiamo al caso $P = P_1 \oplus P_2$. Supponiamo che P_1 e P_2 siano proiettivi; riassumiamo le ipotesi nei seguenti diagrammi (commutativi):



dove i_1 e i_2 sono le immersioni naturali e $\varphi \circ g_1 = f \circ i_1$, $\varphi \circ g_2 = f \circ i_2$. Adesso vogliamo trovare $g : P \longrightarrow M$ tale che $\varphi \circ g = f$. Definendo $g(p_1, p_2) = g_1(p_1) + g_2(p_2)$ $\forall$ $p_1 \in P_1$,

$p_2 \in P_2$, si ha $\varphi(g(p_1,p_2)) = \varphi(g_1(p_1)+g_2(p_2)) = \varphi(g_1(p_1)) + \varphi(g_2(p_2)) = f(i_1(p_1)) + f(i_2(p_2)) = f((p_1,0)) + f((0,p_1)) = f((p_1,p_2))$, e dunque g è il sollevamento cercato.
Viceversa, supponiamo che P sia proiettivo e mostriamo che lo è anche P_1 (per P_2 si procede in maniera analoga). Abbiamo il seguente diagramma:

$$\begin{array}{ccccc} M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \\ {\scriptstyle \exists g}\uparrow & \nwarrow & \uparrow{\scriptstyle f} & & \\ P & \xrightarrow[\pi]{} & P_1 & & \end{array} \qquad \exists ? g_1$$

dove g esiste perché $f \circ \pi : P \longrightarrow N$ e P è proiettivo. Definendo g_1 come $g_1(p_1) = g \circ i_1(p_1)$ $\forall\, p_1 \in P_1$, si ha $\varphi(g_1(p_1)) = \varphi(g(i_1(p_1))) = \varphi(g(p_1,0)) = f(\pi(p_1,0)) = f(p_1)$, da cui $\varphi \circ g_1 = f$ e P_1 è proiettivo.

⋈

Proposizione 2.3.4 *Siano P, M, N e Q A-moduli, allora sono equivalenti i seguenti fatti:*

1. *P è proiettivo;*
2. *Per ogni successione esatta $0 \to M \to N \to Q \to 0$ anche la successione $0 \to Hom(P,M) \to Hom(P,N) \to Hom(P,Q) \to 0$ è esatta;*
3. *Ogni successione esatta del tipo $0 \to M \to N \to P \to 0$ spezza, ovvero $N = M \oplus P$;*
4. *P è addendo diretto di ogni modulo di cui è quoziente, ovvero se $P = M/N$ allora $\exists Q$ t.c $P \oplus Q = M$;*
5. *P è addendo diretto di un modulo libero.*

Dimostrazione:

$1 \Leftrightarrow 2$) Ovvia per definizione;

$1 \Rightarrow 3$) Dato che P è proiettivo, scegliendo $\varphi = id$, consideriamo il seguente grafico:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & & & {\scriptstyle \bar{\varphi}}\uparrow & \nearrow_{\varphi = id} & & & \\ & & & & P & & & & \end{array}$$

dove vale la relazione $g \circ \bar{\varphi} = \varphi = id_P$;

$3 \Rightarrow 4$) Per ipotesi ogni successione del tipo $0 \to N \to M \to P \to 0$ spezza. Se $P = M/N \Rightarrow M = N \oplus P$ e pertanto P è addendo diretto di M di cui è quoziente;

$4 \Rightarrow 5$) Dato che P è addendo diretto di un modulo di cui è quoziente, mi basta far vedere che $P = Q/N$ con Q modulo libero. Consideriamo il seguente A-modulo:

$$A^M = \bigoplus_{m \in M} < m >$$

Per avere una idea su come sia strutturato, un elemento di A^M è una stringa lunga "numero di elementi di M" e in ogni coordinata è presente un elemento che fa parte del generato di un elemento $m \in M$. A^M è un modulo libero (una base è costituita dalle stringhe tutte nulle tranne che in una componente). Consideriamo adesso il morfismo $\psi : A^P \to P$ tale che $\psi(e_p) = p$ (e_p è un elemento della base di A^P al variare di $p \in P$). Il morfismo è suriettivo e pertanto $P = A^P/Ker\psi$;

$5 \Rightarrow 1)$ P addendo diretto di un modulo libero $\Rightarrow P \oplus N = M$ con M libero. Per quanto osservato M è proiettivo perché è libero; allora, per la proposizione dimostrata, P è proiettivo.

$\bowtie$

Definizione 2.31 *Sia M A-modulo, M si dice **iniettivo** se il funtore $Hom(\star, N)$ è esatto anche a destra.*

Proposizione 2.3.5 *Sia A un dominio a ideali principali, allora:*

1. *Ogni $A-$modulo proiettivo è libero;*
2. *Ogni sottomodulo di un modulo proiettivo è proiettivo;*
3. *Ogni sottomodulo di un modulo finitamente generato è finitamente generato.*

Dimostrazione:

1. Sia P proiettivo, allora esistono Q e F $A-$moduli con F libero tali che $P \oplus Q = F$, dunque P è sottomodulo di F e quindi libero.
2. Segue banalmente dal fatto che per gli $A-$moduli, con A PID, proiettivo e libero sono concetti equivalenti.
3. Sia $M = \langle m_1, \cdots, m_n \rangle$ un $A-$modulo finitamente generato, consideriamo la successione esatta:
$$\begin{array}{ccccc} A^n & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\ e_i & \longmapsto & m_i & & \end{array}$$
Sia ora $N \subseteq M$ un sottomodulo e consideriamo $\varphi^{-1}(N) \subseteq A^n$, che è sottomodulo di A^n e dunque è libero di rango $r < n$: sia $\{a_1, \cdots, a_r\}$ una base di $\varphi^{-1}(N)$, allora $\langle \varphi(a_1), \cdots, \varphi(a_r) \rangle = N$ per surgettività e dunque N è finitamente generato.

Capitolo 3

Anelli e moduli di frazioni

3.1 Anelli di frazioni

Dato un anello A, vogliamo costruire un nuovo anello in cui tutti gli elementi di un certo insieme $S \subseteq A$ sono invertibili. Per fare ciò chiediamo che S sia moltiplicativamente chiuso ovvero: $\forall s,t \in S$, $st \in S$ e, inoltre, $1_A \in S$.

ESEMPIO: $S = \{s^n\}_{n\in\mathbb{N}}$, $s \in A$. In particolare, possiamo scegliere $A = \mathbb{Z}$ e $S = \{6^n\}_n$.

ESEMPIO: Sia $P \subseteq A$ ideale primo, $S = A - P$ soddisfa le proprietà che richiediamo: essendo P non banale, $1 \notin P \Rightarrow 1 \in S$, inoltre se $a \notin P, b \notin P \Rightarrow ab \in S$ in quanto P è primo. Possiamo estendere tale costruzione di S come $A - \bigcup_i P_i$ con i P_i primi.

Dato $S \subseteq A$ moltiplicativamente chiuso, definiamo nell'insieme $A \times S$ la relazione:

$$(a,s) \sim (b,t) \quad \Longleftrightarrow \quad \exists u \in S \text{ tale che } u(at - bs) = 0$$

Proposizione 3.1.1 *La relazione sopra introdotta è una relazione di equivalenza.*

Dimostrazione: Le proprietà di riflessione e di simmetria sono banali, dimostriamo la transitività: $(a,s) \sim (b,t)$ e $(b,t) \sim (c,v)$ allora $\exists u, w \in S$ tali che $u(at - bs) = 0$ e $w(bv - ct) = 0$, allora $vwu(at - bs) = 0$ e $usw(bv - ct) = 0$. Sommando membro a membro otteniamo $uwt(av - cs) = 0$. Dunque, scegliendo $r = uwt \in S$ per soddisfare la relazione, si ha che $(a,s) \sim (c,v)$.

⋈

Denotiamo $(A \times S/\sim) = S^{-1}A$ e la classe $[(a,s)] = \frac{a}{s}$. Definiamo una struttura di anello in $S^{-1}A$ mediante le seguenti operazioni definite $\forall \frac{a}{s}, \frac{b}{t} \in S^{-1}A$:

Somma: $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$;

Prodotto: $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$.

Si verifica facilmente che le operazioni sopra introdotte sono ben definite. Inoltre l'elemento neutro per la somma e l'elemento neutro del prodotto sono rispettivamente $\frac{0}{1}$ e $\frac{1}{1}$. Notiamo che in $S^{-1}A$ gli elementi della forma $\frac{s}{1}$ con $s \in S$ sono invertibili e il loro inverso è $\frac{1}{s}$.

Definizione 3.1 *L'anello $S^{-1}A$ è detto* ***anello delle frazioni di A rispetto ad S****.*

ESEMPIO: Se $A = \mathbb{Z}$ e $S = \{6^n\} \Rightarrow S^{-1}\mathbb{Z} = \{\frac{a}{6^n} |\ a \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \mathbb{Q}$.

ESEMPIO: Se $S = A - P$ con P ideale primo, $S^{-1}A = \{\frac{a}{s} |\ a \in A, s \in A - P\}$.

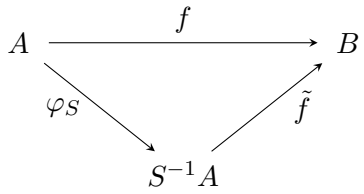
OSSERVAZIONE: Se $0 \in S$, allora $S^{-1}A = 0$ poiché posso sempre scegliere $u = 0$ nella relazione di equivalenza.

Possiamo a questo punto definire la mappa:

$$\begin{array}{rccc} \varphi_S: & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & \frac{a}{1} \end{array}$$

In generale la mappa φ_S non è iniettiva: $a \in Ker\varphi_S \Leftrightarrow \varphi_S(a) = \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists u \in S$ tale che $ua = 0$ $\Leftrightarrow u \in S \cap D(A)$. Pertanto se S interseca i divisori dell'anello, la mappa φ_S non è iniettiva.

Proposizione 3.1.2 (Proprietà universale degli anelli di frazioni) *Siano A, B anelli, $f : A \to B$ un morfismo di anelli e $S \subseteq A$ moltiplicativamente chiuso. Se $f(S) \subseteq B^*$, allora f si fattorizza attraverso l'anello delle frazioni, ovvero $\exists! \tilde{f} : S^{-1}A \to B$ tale che il seguente diagramma è commutativo:*



Dimostrazione: Unicità: Assumiamo che esista $\tilde{f}$, allora $\tilde{f}(\frac{a}{1}) = \tilde{f}(\varphi_S(a)) = f(a)$ e $\tilde{f}(\frac{1}{s}) = \tilde{f}((\frac{s}{1})^{-1}) = \tilde{f}(\frac{s}{1})^{-1} = \tilde{f}(\varphi_S(s)^{-1}) = f(s)^{-1}$. Allora $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$ è univocamente determinato.
Esistenza: Se esiste una tale $\tilde{f}$ deve valere $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. Le verifiche di morfismo discendono banalmente dal fatto che f è un morfismo; verifichiamo invece che $\tilde{f}$ è ben definita, ovvero che se $\frac{a}{s} = \frac{b}{t}$ allora $\tilde{f}(\frac{a}{s}) = \tilde{f}(\frac{b}{t})$: $\frac{a}{s} = \frac{b}{t} \Rightarrow \exists u \in S$ tale che $u(at - bs) = 0 \Rightarrow f(u(at - bs)) = f(u)f(at - bs) = 0$, visto che $f(u) \in B^*$ deve valere $f(at) = f(bs) \Rightarrow f(a)f(s)^{-1} = f(b)f(t)^{-1} \Rightarrow \tilde{f}(\frac{a}{s}) = \tilde{f}(\frac{b}{t})$.

⋈

Proposizione 3.1.3 *Nelle notazioni precedenti, se f è tale che:*

1. *$f(a) = 0 \Rightarrow \exists u \in S$ tale che $ua = 0$;*
2. *Per ogni $b \in B$ esistono $a \in A, s \in S$ tali che $b = f(a)f(s)^{-1}$;*

allora $\tilde{f}$ è un isomorfismo.

Dimostrazione: La suriettività deriva direttamente dalla seconda condizione. Per l'iniettività, sia $\frac{a}{s} \in Ker\tilde{f} \Rightarrow \tilde{f}(\frac{a}{s}) = 0 \Rightarrow f(a)f(s)^{-1} = 0 \Rightarrow f(a) = 0$ in quanto $f(s) \in B^*$. Allora, per la prima condizione, esiste $u \in S$ tale che $ua = 0 \Rightarrow a \in Ker\varphi_S$ ovvero $\frac{a}{s} = \frac{0}{1}$.

Definizione 3.2 *Sia A anello, $S \subseteq A$, $S = \{s^n\}$ con $s \notin \mathcal{N}(A)$, denotiamo $S^{-1}A = A_s = \{\frac{a}{s^n} |\ a \in A, n \in \mathbb{N}\}$*

Definizione 3.3 *Sia A anello e P ideale primo, $S = A - P$, diciamo che $S^{-1}A = A_P$ è una* ***localizzazione di A in P****.*

Esempio: $A = \mathbb{Z}$, $S = \{2^n\}$, allora $\mathbb{Z}_2 = \{\frac{a}{2^k} |\ a \in \mathbb{Z}\}$. Se invece $S = \mathbb{Z} - (2)$ allora $Z_{(2)} = \{\frac{a}{s} |\ a \in \mathbb{Z}, 2 \text{ non divide } s\}$

Proposizione 3.1.4 *Sia A anello, P ideale primo di A, allora A_P è locale con ideale massimale $M = \{\frac{a}{s} |\ a \in P, s \notin P\}$.*

Dimostrazione: Il fatto che M sia un ideale è una semplice verifica. Notiamo inoltre che $M \neq A_P$ infatti se $\frac{1}{1} \in M \Rightarrow \exists \frac{a}{s} \in M$ tale che $\frac{a}{s} = \frac{1}{1} \Rightarrow \exists u \in S$ tale che $u(a-s) = 0 \Rightarrow P \ni ua = us \notin P$ assurdo. Mostriamo che ogni elemento che non appartiene a M è invertibile: se $\frac{a}{s} \notin M \Rightarrow a \notin P, s \notin P \Rightarrow \frac{s}{a} \in A_P \Rightarrow \frac{a}{s} \in A_P^*$.

⋈

Vogliamo adesso studiare gli ideali di $S^{-1}A$. Partiamo dalla mappa $\varphi_S : A \to S^{-1}A$ e vediamo, a partire da un ideale $I \subseteq A$ chi è I^e: $I^e = (\varphi_S(I)) = \{\sum_{i=1}^n \frac{a_i}{s_i}\frac{b_i}{1} |\ a_i \in A, s_i \in S, b_i \in I\} = \{\sum_{i=1}^n \frac{a_i b_i}{s_i} |\ a_i \in A, s_i \in S, b_i \in I\} = \{\frac{\sum_{i=1}^n t_i a_i b_i}{s}\ a_i \in A, s = \prod_{i=1}^n s_i, t_i = \frac{s}{s_i}, b_i \in I\}$ e visto che il numeratore appartiene a I e il denominatore a S allora $I^e \subseteq S^{-1}I = \{\frac{i}{v} |\ i \in I, v \in S\}$. Mostriamo anche l'altro contenimento: sia $\frac{i}{s} \in S^{-1}I$, vediamo $\frac{i}{s} = \frac{i}{1}\frac{1}{s}$ dove $\frac{i}{1} \in I^e \Rightarrow \frac{i}{s} \in I^e$. Abbiamo pertanto mostrato la seguente:

Proposizione 3.1.5 *Sia A anello, I ideale di A, $\varphi_S : A \to S^{-1}A$, allora $I^e = S^{-1}I$.*

Dimostrazione: Già fatta.

⋈

Proposizione 3.1.6 *Sia A anello, I ideale di A, $\varphi_S : A \to S^{-1}A$, allora $S^{-1}I = S^{-1}A$ se e solo se $I \cap S \neq \emptyset$.*

Dimostrazione: $\Rightarrow$)Se $S^{-1}I = S^{-1}A \Rightarrow \exists \frac{a}{b} \in S^{-1}I$ invertibile, ovvero $\exists \frac{b}{t} \in S^{-1}A$ tale che $\frac{ab}{st} = \frac{1}{1} \Rightarrow \exists u \in S$ tale che $uab = ust$, ma allora il membro di sinistra appartiene a I, quello di destra a S e quindi $uab \in S \cap I$;
$\Leftarrow$)Sia $i \in I \cap S \Rightarrow \varphi_S(i) = \frac{i}{1} \in S^{-1}I$ e $\frac{i}{1} \in (S^{-1}A)^* \Rightarrow S^{-1}I = S^{-1}A$.

⋈

Vogliamo adesso mostrare che ogni ideale di $S^{-1}A$ è un ideale esteso mediante il solito morfismo φ_S, e cioè che $\forall J \subseteq S^{-1}A$ esiste $I \subseteq A$ tale che $I^e = J$. Mostriamo che per ogni ideale $J \subseteq S^{-1}A$, $J^{ce} = J$. In generale abbiamo il contenimento $J^{ce} \subseteq J$. Proviamo l'altro: $\frac{a}{s} \in J \Rightarrow \frac{s}{1}\frac{a}{s} = \frac{a}{1} \in J \Rightarrow a \in J^c \Rightarrow \frac{a}{1} \in J^{ce} \Rightarrow \frac{a}{1}\frac{1}{s} = \frac{a}{s} \in J^{ce}$. Dato che vale l'uguaglianza $J = J^{ce}$ ogni ideale J lo possiamo scrivere come $S^{-1}(J^c)$ che è proprio quello che volevamo mostrare.

Proposizione 3.1.7 *Sia A anello, I ideale di A, $\varphi_S : A \to S^{-1}A$, allora $I^{ec} = \bigcup_{s \in S}(I : s)$;*

Dimostrazione: Se $x \in I^{ec} = (S^{-1}I)^c \Rightarrow \frac{x}{1} = \frac{a}{s}$ con $a \in I \Rightarrow \exists u \in S$ tale che $u(xs - a) = 0 \Rightarrow I \ni ua = uxs \Rightarrow x \in (I : us) \Rightarrow x \in \bigcup_{s \in S}(I : s)$. Viceversa se $x \in \bigcup_{s \in S}(I : s) \Rightarrow \exists s \in S$ tale che $xs = i$ con $i \in I \Rightarrow \frac{xs}{1} = \frac{i}{1} \Rightarrow \frac{x}{1} = \frac{i}{s} \Rightarrow \frac{x}{1} \in I^e \Rightarrow x \in I^{ec}$.

⋈

Proposizione 3.1.8 *Sia $P \subseteq A$ ideale, prendiamo $S \subseteq A$ moltiplicativamente chiuso e $P \cap S = \emptyset$, allora P è primo se e solo se $S^{-1}P$ è primo.*

Dimostrazione: $\Rightarrow$)Sia $\frac{a}{s}\frac{b}{t} \in S^{-1}P \Rightarrow \exists p \in P$ tale che $\frac{ab}{st} = \frac{p}{v} \Rightarrow \exists u \in S$ tale che $u(abv - pst) = 0 \Rightarrow uvab = upst$. Dato che $upst \in P$ e $P \cap S = \emptyset \Rightarrow ab \in P \Rightarrow a \in P$ o $b \in P \Rightarrow \frac{a}{s} \in S^{-1}P$ o $\frac{b}{t} \in S^{-1}P$;
$\Leftarrow$)Sia $ab \in P \Rightarrow \frac{ab}{1} = \frac{a}{1}\frac{b}{1} \in S^{-1}P$ primo, allora, senza perdita di generalità, supponiamo $\frac{a}{1} \in S^{-1}P \Rightarrow \frac{a}{1} = \frac{p}{s}$ con $p \in P$. Esiste dunque $u \in S$ tale che $uas = up \in P \Rightarrow uas \in P$, ma $us \notin P$ poiché in S e dunque $a \in P$.

⋈

La proposizione precedente mostra l'esistenza di una corrispondenza $1:1$ tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A tali che $A \cap S = \emptyset$.

Proposizione 3.1.9 (Proprietà di S^{-1}) *Per ogni ideale $I, J \in A$ vale che:*

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

Dimostrazione:

1. $\subseteq$) $\frac{a}{s} \in S^{-1}(I+J) \Rightarrow \exists i \in I, j \in J$ tali che $\frac{a}{s} = \frac{i+j}{s} = \frac{i}{s} + \frac{j}{s} \in S^{-1}I + S^{-1}J$;
   $\supseteq$) $\frac{i}{s} + \frac{j}{t} \in S^{-1}I + S^{-1}J \Rightarrow \frac{i}{s} + \frac{j}{t} = \frac{it+js}{st} \in S^{-1}(I+J)$
2. $\subseteq$) $\frac{a}{s} \in S^{-1}(I \cap J) \Rightarrow \frac{a}{s} \in S^{-1}I$ e $\frac{a}{s} \in S^{-1}J \Rightarrow \frac{a}{s} \in S^{-1}I \cap S^{-1}J$;
   $\supseteq$) $\alpha \in S^{-1}I \cap S^{-1}J \Rightarrow \alpha = \frac{a}{s} = \frac{b}{t}$ con $a \in I, b \in J \Rightarrow \exists u \in S$ tale che $u(at - bs) = 0 \Rightarrow uat = ubs \in I \cap J$ poiché il membro di sinistra appartiene a I e quello di destra appartiene a J. Allora $\frac{a}{s} = \frac{uta}{uts} \in S^{-1}(I \cap J)$;
3. $\subseteq$) In generale vale che $(\sqrt{I})^e \subseteq \sqrt{I^e}$ e pertanto si ha il contenimento $S^{-1}\sqrt{J} \subseteq \sqrt{S^{-1}J}$;
   $\supseteq$) $\frac{a}{s} \in \sqrt{S^{-1}I} \Rightarrow \exists n \in \mathbb{N}$ tale che $\frac{a^n}{s^n} \in S^{-1}I \Rightarrow \frac{a^n}{s^n} = \frac{i}{t}$ con $i \in I \Rightarrow \exists u \in S$ tale che $u(a^n t - is^n) = 0 \Rightarrow uta^n = uis^n \Rightarrow uta^n \in I$ poiché il membro di destra appartiene a $I \Rightarrow (uta)^n \in I \Rightarrow uta \in \sqrt{I}$. Allora $\frac{a}{s} = \frac{uta}{uts} \in S^{-1}\sqrt{I}$.

⋈

Preso M un A-modulo, sia $S \subseteq A$ moltiplicativamente chiuso, allora consideriamo $M \times S/\sim$ con $\sim$ relazione di equivalenza definita analogamente nel caso degli anelli.

Definizione 3.4 *Definiamo $(M \times S/\sim) = S^{-1}M$* ***localizzazione del modulo rispetto a S.***

Con le seguenti operazioni $S^{-1}M$ risulta essere un $S^{-1}A$-modulo:

Somma: $\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$, $\forall \frac{m}{s}, \frac{n}{t} \in S^{-1}M$;

Prodotto esterno: $\frac{a}{s}\frac{m}{t} = \frac{am}{st}$, $\forall \frac{a}{s} \in S^{-1}A, \forall \frac{m}{t} \in S^{-1}M$.

È facile verificare che le operazioni introdotte sono ben definite.
Data $f : M \to N$ morfismo di A-moduli, nelle notazioni precedenti, è ben definita la mappa

$$\begin{array}{rccc} S^{-1}f: & S^{-1}M & \longrightarrow & S^{-1}N \\ & \frac{m}{s} & \longmapsto & \frac{f(m)}{s} \end{array}$$

infatti: se $\frac{m}{s} = \frac{n}{t} \Rightarrow \exists u \in S$ tale che $u(mt - ns) = 0 \Rightarrow uf(mt - ns) = 0 \Rightarrow utf(m) - usf(n) = 0$ poiché $u, s, t \in A$, allora $u(tf(m) - sf(n)) = 0 \Rightarrow \frac{f(m)}{s} = \frac{f(n)}{t}$.

Lemma 3.1.10 *Date $f : N \to M$, $g : M \to P$ morfismi di A-moduli, allora $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$.*

Dimostrazione: $S^{-1}(g \circ f)(\frac{n}{s}) = \frac{(g \circ f)(n)}{s} = \frac{g(f(n))}{s} = S^{-1}g(\frac{f(n)}{s}) = S^{-1}g((S^{-1}(f))(\frac{n}{s})) = (S^{-1}g \circ S^{-1}f)(\frac{n}{s})$.

⋈

Proposizione 3.1.11 *Data la successione esatta $N \xrightarrow{f} M \xrightarrow{g} P$, allora la successione $S^{-1}N \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}P$ è esatta.*

Dimostrazione: La tesi è equivalente a mostrare che $ImS^{-1}f = KerS^{-1}g$. Facciamo vedere i due contenimenti:
$\subseteq$) Per ipotesi $Imf = Kerg \Rightarrow g \circ f = 0 \Rightarrow S^{-1}(g \circ f) = \frac{0}{1} = S^{-1}g \circ S^{-1}f \Rightarrow ImS^{-1}f \subseteq KerS^{-1}g$
$\supseteq$) Sia $\frac{m}{s}$ t.c $S^{-1}g(\frac{m}{s}) = \frac{g(m)}{s} = \frac{0}{1}$ allora $\exists u \in S$ t.c $ug(m) = 0 = g(um) \Rightarrow um \in Kerg = Imf \Rightarrow$ $\exists n \in N$ t.c. $um = f(n)$ allora $\frac{m}{s} = \frac{um}{us} = \frac{f(n)}{us} \in ImS^{-1}f$.

$\bowtie$

OSSERVAZIONE: Per quanto appena visto, S^{-1} risulta essere un funtore tra la categoria degli A moduli a quella degli $S^{-1}A$ moduli. In particolare S^{-1} è un funtore covariante esatto.

Proposizione 3.1.12 *Dati M, N sottomoduli di un A-modulo P valgono le seguenti proprietà:*

1. $S^{-1}(M + N) = S^{-1}M + S^{-1}N$;
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$;
3. *Se $N \subseteq M$,* $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Dimostrazione: $1, 2$ analoghe a quelle viste con gli ideali. Per la terza proprietà consideriamo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}N & \xrightarrow{S^{-1}i} & S^{-1}M & \xrightarrow{S^{-1}\pi} & S^{-1}(M/N) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & S^{-1}N & \xrightarrow[\tilde{i}]{} & S^{-1}M & \xrightarrow[\tilde{\pi}]{} & S^{-1}M/S^{-1}N & \longrightarrow & 0 \end{array}$$

dove la prima successione esatta corta è ottenuta applicando alla successione sotto indicata il funtore esatto S^{-1}:

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

La tesi segue dal lemma del serpente.

$\bowtie$

La prossima proposizione si trova nei libri di testo con un uguale, ma con la dimostrazione fornita siamo in grado solamente di mettere un isomorfismo:

Proposizione 3.1.13 *Siano $M, N \subseteq P$ A-moduli con N finitamente generato, allora* $S^{-1}(M : N) \cong (S^{-1}M : S^{-1}N)$.

Dimostrazione: Osserviamo che la tesi è equivalente a mostrare che $S^{-1}(Ann(N)) \cong Ann(S^{-1}N)$, infatti: $S^{-1}(M : N) = S^{-1}(Ann((M + N)/M)) \cong Ann(S^{-1}(M + N/M)) = Ann(S^{-1}(M + N)/S^{-1}M) = Ann((S^{-1}M + S^{-1}N)/S^{-1}M) = S^{-1}M : S^{-1}N$. Mostriamo dunque per induzione sul numero di generatori di N che $S^{-1}(Ann(N)) \cong Ann(S^{-1}N)$:
Passo base $n = 1$) $N =< m >$ con $m \neq 0$, allora $\exists \varphi : A \to N$ morfismo suriettivo tale che $\varphi(a) = am$. $Ker\varphi = \{a \in A | \ am = 0\} = Ann(N) \Rightarrow N \cong A/Ann(N)$. Applicando il funtore S^{-1} si ottiene $S^{-1}N \cong S^{-1}(A/Ann(N)) \cong S^{-1}A/S^{-1}(Ann(N))$. Consideriamo adesso $S^{-1}N$: questo è un $S^{-1}A$-modulo finitamente generato e dunque, ragionando come sopra, esiste $f : S^{-1}A \to$

$S^{-1}N$ suriettiva tale che $f(\frac{a}{1}) = \frac{am}{1}$. Analogamente a sopra si mostra che $Kerf = Ann(S^{-1}N)$. Possiamo pertanto considerare la seguente situazione:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}(Ann(N)) & \xrightarrow{S^{-1}i} & S^{-1}A & \xrightarrow{S^{-1}\varphi} & S^{-1}N & \longrightarrow & 0 \\ & & \downarrow g & & \downarrow id & & \downarrow id & & \\ 0 & \longrightarrow & Ann(S^{-1}N) & \xrightarrow[\tilde{i}]{} & S^{-1}A & \xrightarrow[f]{} & S^{-1}N & \longrightarrow & 0 \end{array}$$

Possiamo dunque concludere che $S^{-1}(Ann(N)) \cong Ann(S^{-1}N)$ applicando il lemma del serpente; Passo induttivo $n \Rightarrow n+1$) Sia N generato da $n+1$ elementi, $N = N_1 + N_2$ con N_1, N_2 finitamente generati con un numero inferiore di generatori (per cui vale quindi l'ipotesi induttiva). Allora $S^{-1}(Ann(N)) = S^{-1}(Ann(N_1 + N_2)) = S^{-1}(Ann(N_1) \cap Ann(N_2)) \cong S^{-1}(Ann(N_1)) \cap S^{-1}(Ann(N_2)) = Ann(S^{-1}N_1) \cap Ann(S^{-1}N_2) = Ann(S^{-1}N_1 + S^{-1}N_2) = Ann(S^{-1}N)$.

⋈

Osservazione: L'ipotesi che N sia finitamente generato è necessaria per il teorema. Supponiamo infatti $A = \mathbb{K}[x, t, \frac{x}{t}, \frac{x}{t^2}, ...]$, $I = (x)$, $J = (\frac{x}{t}, \frac{x}{t^2}, ...)$, $S^{\{}t^n\}$. Allora $I : J = I \Rightarrow S^{-1}(I : J) = S^{-1}I$, ma $S^{-1}I \supseteq (\frac{x}{t}, \frac{x}{t^2}, ...) = J \Rightarrow S^{-1}I : S^{-1}J = S^{-1}A$ che è diverso da $S^{-1}I$ (è un ideale proprio).

Definizione 3.5 *Una proprietà $\mathcal{P}$ si dice **locale** in un anello A (o in un A-modulo M) se vale: $\mathcal{P}$ è vera per A (M) $\Leftrightarrow \forall P \subseteq A$ primo $\mathcal{P}$ è vera per A_P (M_P)*

Alcuni esempi di proprietà locali sono l'essere nullo, l'iniettività e la surgettività di un morfismo:

Proposizione 3.1.14 *Sia M un A-modulo, sono fatti equivalenti:*

1. *$M = 0$;*
2. *$M_P = 0 \ \forall P \subseteq A$ ideale primo;*
3. *$M_P = 0 \ \forall P \subseteq A$ ideale massimale.*

Dimostrazione: Le implicazioni $1 \Rightarrow 2$, $1 \Rightarrow 3$ e $2 \Rightarrow 3$ sono banali. Facciamo vedere che $3 \Rightarrow 1$: supponiamo che esista un $0 \neq m \in M$: se $Ann(m)$ è un ideale proprio eisiste un ideale $N \subseteq A$ massimale t.c. $Ann(m) \subseteq N$, inoltre, per ipotesi, $M_N = 0$ allora $\frac{m}{1} = \frac{0}{1} \Rightarrow \exists s \notin N$ (l'insieme moltiplicativo è in questo caso $A - N$) t.c. $sm = 0 \Rightarrow s \in Ann(m)$ ma questo è assurdo; se invece l'annullatore di m è vuoto non potrà mai valere $sm = 0$ per un certo s dell'insieme moltiplicativo, assurdo dato che deve valere $M_N = 0$.

⋈

Proposizione 3.1.15 *Dato $\varphi : M \to N$ omomorfismo di A-moduli, sono fatti equivalenti:*

1. *φ è inietttivo (surgettivo);*
2. *$S^{-1}\varphi : M_P \to N_P$, con $S = A - P$ e $\forall P \subseteq A$ ideale primo, è iniettiva (surgettiva);*
3. *$S^{-1}\varphi : M_L \to N_L$, con $S = A - L$ e $\forall L \subseteq A$ ideale massimale, è iniettiva (surgettiva);*

Dimostrazione: L'unica implicazione interessante è $3 \Rightarrow 1$: la successione $0 \longrightarrow Ker\varphi \longrightarrow M \xrightarrow{\varphi} N$ è esatta, allora (applicando il funto S^{-1})sappiamo che anche $0 \longrightarrow (Ker\varphi)_L \longrightarrow M_L \xrightarrow{S^{-1}\varphi} N_L$ è esatta, e ciò implica (usando l'ipotesi di iniettività) che $(Ker\varphi)_L = 0 \ \forall L \subseteq A$ massimale; la tesi segue dalla proposizione precedente. Per quanto riguarda la suriettività si ragiona in modo analogo.

$\bowtie$

Proposizione 3.1.16 *Essere ridotto è una proprietà locale.*

Dimostrazione: Sappiamo che S^{-1} commuta col passaggio al radicale: si ha infatti $S^{-1}\sqrt{0} = \sqrt{S^{-1}0}$, da cui $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$. Si ha dunque la tesi.

$\bowtie$

Per costruzione, nell'anello $S^{-1}A$, tutti gli elementi di S sono invertibili; ci chiediamo se sono tutti e soli: per esempio, prendendo $A = \mathbb{Z}$ e $S = \{6^n\}$, $S^{-1}A = \mathbb{Z}_6 = \{\frac{a}{6^n} |\ a \in \mathbb{Z}\}$, $\frac{2}{1}\frac{3}{6} = \frac{1}{1}$ e pertanto anche l'elemento 2 è invertibile in $\mathbb{Z}_6$; allo stesso modo si mostra che anche 3 invertibile e così tutte le potenze di 2 e di 3.

Definizione 3.6 *Un insieme T moltiplicativamente chiuso si dice* ***saturato*** *se per ogni $xy \in T \Rightarrow x \in T$ e $y \in T$.*

Osservazione: Nell'esempio precedente l'insieme $S = \{6^n\}$ non è saturato.

Proposizione 3.1.17 *Siano A un anello e $U = \{a \in A \mid \frac{a}{1}$ è invertibile in $T^{-1}A\}$ con $T \subseteq A$ sottoinsieme moltiplicativo saturato, allora $T = U$.*

Dimostrazione: Mostriamo le due inclusioni:
$\subseteq$) Già vista.
$\supseteq$) Se $a \in U \Rightarrow \exists\ \frac{b}{t} \in T^{-1}A$ t.c $\frac{a}{1}\frac{b}{t} = \frac{1}{1} \Rightarrow \exists u \in T$ t.c $uab = ut \in T \Rightarrow a \in T$ in quanto T è saturato.

$\bowtie$

Proposizione 3.1.18 *Sia A un anello, allora $T \subseteq A$ è saturato $\Leftrightarrow T = A - \bigcup_{P\ primo} P$*

Dimostrazione:
$\Leftarrow$) Mostriamo innanzitutto che $T = A - \bigcup_{P\ primo} P$ è un insieme moltiplicativo: $1 \in T$ poichè $1 \notin P$ per ogni ideale primo (proprio), inoltre se $s, t \in T$ allora $s, t \notin P \Rightarrow st \notin P$ per ogni primo dell'unione, dunque $st \in T$. Mostriamo ora che T è saturato: $st \in T \Leftrightarrow st \notin P \Rightarrow s \notin P$ e $t \notin P$ per ogni primo dell'unione, dunque $s \in T$ e $t \in T$.
$\Rightarrow$) Sia T saturato e consideriamo l'insieme $A - \bigcup_{P\ primo} P$ con $P \cap T = \emptyset$. Vogliamo mostrare che $T = A - \bigcup_{P\ primo} P$. Ovviamente vale che $T \subseteq A - \bigcup_{P\ primo} P$. Mostriamo l'altro contenimento con la contronominale: sia $s \notin T \Rightarrow \frac{s}{1}$ non è invertibile per la proposizione precedente $\Rightarrow M \subseteq T^{-1}A$ ideale massimale tale che $\frac{s}{1} \in M$. L'ideale M è massimale e dunque primo e, per la caratterizzazione degli ideali primi in $T^{-1}A$, $M = T^{-1}P$ con P ideale primo di A tale che $P \cap T = \emptyset$. Dunque $\frac{s}{1} = \frac{a}{t}$ con $a \in P, t \in T \Rightarrow \exists u \in T$ tale che $ust = ua \Rightarrow ust \in P \Rightarrow s \in P$ che è la tesi.

$\bowtie$

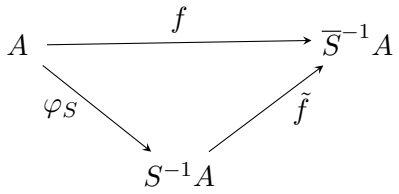
Definizione 3.7 *Siano A un anello e $S \subseteq A$ sottoinsieme moltiplicativo, definiamo $\overline{S} = \{a \in A \mid \exists b \in A$ t.c. $ab \in S\}$* ***saturato di*** *S.*

Teorema 3.1.19 *Sia S sottoinsieme moltiplicativo di un anello A, allora:*

1. **a)** $S \subseteq \overline{S}$;
   b) $\overline{S}$ *è saturato;*
   c) *Sia* $T \subseteq A$ *saturato, se* $T \supseteq S \Rightarrow T \supseteq \overline{S}$;
2. *Sia* $U = (S^{-1}A)^* \Rightarrow U = \{\frac{a}{s} |\ a \in \overline{S}, s \in S\}$;
3. $\overline{S} = A - \bigcup_{P\ primi} P$ *tali che* $P \cap S = \emptyset$;
4. $S^{-1}A = \overline{S}^{-1}A$.

Dimostrazione:

1. **a)** Sia $s \in S \Rightarrow 1s \in S \Rightarrow s \in \overline{S}$;
   b) Per quanto visto $S \subseteq \overline{S} \Rightarrow 1 \in \overline{S}$. Siano adesso $a, b \in \overline{S} \Rightarrow \exists s, t \in A$ tali che $as \in S, bt \in S \Rightarrow (as)(bt) = (ab)(st) \in S \Rightarrow ab \in \overline{S}$. Sia adesso $ab \in \overline{S} \Rightarrow \exists u \in A$ tale che $u(ab) \in S \Rightarrow a(ub) \in S, b(ua) \in S \Rightarrow a, b \in \overline{S}$;
   c) Sia $a \in \overline{S} \Rightarrow \exists u \in A$ tale che $au \in S \subseteq T \Rightarrow a \in T$ poiché T è saturato;
2. $\subseteq$) Sia $\frac{a}{s} \in U$ con $s \in S$. Ci basta mostrare che $a \in \overline{S}$. Per ipotesi $\exists \frac{b}{t} \in S^{-1}A$ tale che $\frac{a}{s}\frac{b}{t} = \frac{1}{1} \Leftrightarrow \exists u \in S$ t.c. $uab = ust$; adesso $ust \in S \Rightarrow a(ub) \in S \Rightarrow a \in \overline{S}$;
   $\supseteq$) Sia $\frac{a}{s}$ con $a \in \overline{S}, s \in S \Rightarrow \exists b \in A$ tale che $ab \in S$; ma allora $\frac{a}{s} = \frac{ab}{bs}$ è invertibile in $S^{-1}A$ con inverso $\frac{bs}{ab}$;
3. Per non appesantire la notazione indichiamo con P un ideale primo. $\overline{S} = A - \bigcup_{P \cap \overline{S} = \emptyset} P$; si ha il contenimento insiemistico $A - \bigcup_{P \cap \overline{S} = \emptyset} P \supseteq A - \bigcup_{P \cap S = \emptyset} P$ ragionando sulle intersezioni. Per l'altro contenimento osserviamo che $A - \bigcup_{P \cap S = \emptyset} P$ è un insieme saturato che contiene S e pertanto $A - \bigcup_{P \cap \overline{S} = \emptyset} P \supseteq \overline{S} = A - \bigcup_{P \cap \overline{S} = \emptyset} P$
4. Utilizziamo la proprietà fondamentale degli anelli di frazioni: consideriamo pertanto il grafico:



   con $f = \varphi_{\overline{S}}$, ovvero $f(a) = \frac{a}{1}$. Se dimostriamo che:
   1) $\forall s \in S$, $f(s) \in (\overline{S}^{-1}A)^*$;
   2) $\forall a \in A$, se $f(a) = 0 \Rightarrow \exists u \in S$ tale che $ua = 0$;
   3) $\forall \alpha \in \overline{S}^{-1}A$, $\alpha = f(a)f(s)^{-1}$ con $a \in A, s \in S$
   allora la tesi segue per la proprietà universale e $S^{-1}A = \overline{S}^{-1}A$ tramite $\tilde{f}$. Dimostriamo dunque i tre punti:
   1) Ovvio per costruzione;
   2) Sia a tale che $f(a) = \frac{a}{1} = \frac{0}{1} \Rightarrow \exists t \in \overline{S}$ tale che $at = 0$ e $\exists b \in A$ tale che $bt \in S$. Allora $atb = 0$ e chiamando $bt = u$ si ha la tesi;
   3) Sia $\alpha \in \overline{S}^{-1}A$, $\alpha = \frac{b}{t}$ con $t \in \overline{S}$. Proviamo che l'elemento $\frac{t}{1}$ è invertibile in $S^{-1}A$: supponiamo che non lo sia, allora (come nella proposizione precedente) $\frac{t}{1} \in S^{-1}P$ con P ideale primo e $P \cap S = \emptyset$ e quindi (sempre come sopra) $t \in P$, ma $t \in \overline{S} = A - \bigcup_{P \cap S = \emptyset}$, assurdo. Dunque $\frac{t}{1}$ è invertibile, cioè $\exists \frac{c}{v}$ con $v \in S$ tale che $\frac{t}{1}\frac{c}{v} = \frac{1}{1}$. Adesso $\alpha = \frac{b}{t} = \frac{b}{t}\frac{t}{1}\frac{c}{v} = \frac{bc}{v} = f(bc)f(v)^{-1}$ che è la tesi.

$\bowtie$

Capitolo 4

Prodotto tensoriale

Definizione 4.1 *Siano M, N, e P A-moduli, definiamo $f : M \times N \to P$* ***applicazione bilineare di A-moduli*** *se le mappe $F_m : N \to P$ t.c $F_m(n) = f(m,n)$ e $F_n : M \to P$ t.c $F_n(m) = f(m,n)$ sono omomorfismi di A-moduli.*

Definizione 4.2 *Date le applicazioni bilineari di A-moduli $f, g : M \times N \to P$ definiamo le operazioni:*
Somma: $(f+g)(m,n) = f(m,n) + g(m,n)\ \forall (m,n) \in M \times N$
Prodotto esterno: $(af)(m,n) = af(m,n)\ \forall a \in A,\ \forall (m,n) \in M \times N$
Si verifica facilmente che, dotato di tali operazioni, $Bil(M,N,P)$ (o anche $L^2(M,N,P)$) è un A-modulo.

OSSERVAZIONE: Segue banalmente dalla definizione che per ogni $f : M \times N \to P$ forma bilineare di A-moduli e per ogni $a \in A$, $af(m,n) = f(am,n) = f(m,an)$.

Proposizione 4.0.1 *Siano M, N e P A-moduli, allora $Bil(M,N,P) \cong Hom_A(M, Hom_A(N,P))$ come A-moduli.*

Dimostrazione: Consideriamo la seguente applicazione e mostriamo che è un isomorfismo:

$$\begin{array}{rccccccccc} \varphi : & Bil(M,N,P) & \longrightarrow & Hom_A(M, Hom_A(N,P)) & & & & & & \\ & f & \longmapsto & g_f : & M & \longrightarrow & Hom_A(N,P) & & & \\ & & & & m & \longmapsto & F_m : & N & \longrightarrow & P \\ & & & & & & & n & \longmapsto & f(m,n) \end{array}$$

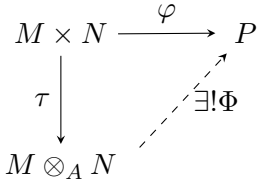
Morfismo: $\forall m \in M, \forall n \in N, \forall f_1, f_2 \in Bil(M,N,P)$ vale che $\varphi(f_1+f_2)(m)(n) = (f_1 + f_2)(m,n) = f_1(m,n) + f_2(m,n) = \varphi(f_1)(m)(n) + \varphi(f_2)(m)(n)$
Inoltre $\forall m \in M, \forall n \in N, \forall a \in A, \forall f \in Bil(M,N,P)$ vale che $\varphi(af)(m)(n) = f(am,n) = af(m,n) = a\varphi(f)(m)(n)$;

Iniettività: Sia $f \in Ker\varphi \Rightarrow g_f = 0 \Rightarrow f(m,n) = 0\ \forall m \in M, \forall n \in N \Rightarrow f = 0$

Suriettività: Sia $h \in Hom_A(M, Hom_A(N,P))$, allora $\forall m \in M, \forall n \in N\ h(m)(n) = \eta(m,n)$ (posso farlo per la definizione di bilinearità). Allora basta scegliere $\eta \in Bil(M,N,P)$ per avere la tesi.

Definizione 4.3 *Sia A anello, M, N A-moduli; si definisce* ***prodotto tensoriale****, un modulo $M \otimes_A N$ e una applicazione bilineare $\tau : M \times N \to M \otimes_A N$ con $\tau(m,n) = m \otimes_A n$ tale che*

$\forall \varphi : M \times N \to P$ *forma bilineare esiste unico* $\Phi : M \otimes_A N \to P$ *morfismo di A-moduli che fa commutare il seguente diagramma:*



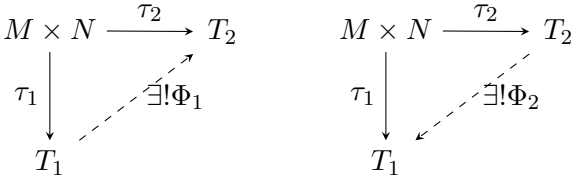
La proprietà della definizione viene usualmente chiamata proprietà universale del prodotto tensoriale.

Se non ci sono ambiguità riguardo all'anello sul quale si sta tensorizzando indicheremo $M \otimes_A N$ con $M \otimes N$ e $m \otimes_A n$ con $m \otimes n$.

Teorema 4.0.2 *Sia A anello, M, N A-moduli; allora il prodotto tensoriale* $M \otimes_A N$ *esiste ed è unico.*

Dimostrazione:

Unicità: Supponiamo che (T_1, τ_1) e (T_2, τ_2) siano due prodotti tensoriali distinti degli A-moduli M, N. Consideriamo allora i seguenti grafici:

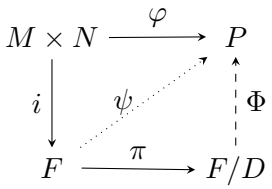


Grazie alla proprietà universale del prodotto tensoriale si ha che $\Phi_1 \circ \tau_1 = \tau_2$ e che $\Phi_2 \circ \tau_2 = \tau_1$. Sostituendo la seconda alla prima e poi la prima alla seconda si ottiene $\Phi_1 \circ \Phi_2 = \Phi_2 \circ \Phi_1 = id$ cioè Φ_1 è un isomorfismo.

Esistenza: Per mostrare l'esistenza di questa struttura definiamo un quoziente e verifichiamo che soddisfa la proprietà universale: consideriamo l'anello $F = A^{M \times N}$ come è già stato definito nella dimostrazione dei moduli proiettivi e consideriamo la mappa

$$\begin{array}{rccccc} \tau : & M \times N & \xrightarrow{i} & F & \xrightarrow{\pi} & F/D \\ & (m,n) & \to & e_{(m,n)} & \to & \overline{e_{(m,n)}} \end{array}$$

con $D =< i(m_1+m_2,n)-i(m_1,n)-i(m_2,n), i(am,n)-ai(m,n), i(m,n_1+n_2)-i(m,n_1)-i(m,n_2), i(m,an)-ai(m,n) >$ al variare di $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ e $a \in A$. Vorremmo adesso mostrare che F/D è effettivamente $M \otimes N$. Consideriamo il seguente grafico per ogni A-modulo P e per ogni $\varphi \in Bil(M, N, P)$:



Se mostriamo che esiste un'unica Φ tale che $\Phi \circ \pi \circ i = \Phi \circ \tau = \varphi$ abbiamo finito. Dato che F è libero $\exists! \psi : F \to P$ tale che $\psi(i(m,n)) = \varphi(m,n)$. Se adesso esiste Φ tale che $\Phi \circ \pi = \psi$, allora Φ è unica e $\Phi \circ \tau = \Phi \circ \pi \circ i = \psi \circ i = \varphi$. Definiamo dunque

$$\begin{array}{rccc} \Phi: & F/D & \longrightarrow & P \\ & \bar{x} & \longmapsto & \psi(x) \end{array}$$

Grazie alla definizione di D l'applicazione Φ è ben definita: sia $\bar{x} = \bar{y}$, dobbiamo mostrare che $\Phi(\bar{x}) = \Phi(\bar{y})$ o equivalentemente che se $x - y \in D \Rightarrow \psi(x-y) = 0$, ovvero che se $a \in D \Rightarrow \psi(a) = 0$. Se $a \in D \Rightarrow a = k_1 r_1 + k_2 r_2 + k_3 r_3 + k_4 r_4$ con $k_i \in A$ e r_i relazioni che generano D. $\psi(a) = k_1(\psi(i(m_1+m_2,n)) - \psi(i(m_1,n)) - \psi(i(m_2,n))) + ... = k_1(\phi(m_1+m_2,n) - \phi(m_1,n) - \phi(m_2,n)) + ... = 0$. L'applicazione Φ è un morfismo (discende da ψ) e pertanto si ha la tesi.

$\bowtie$

Definizione 4.4 *Dato $M \otimes_A N$ prodotto tensoriale, gli elementi della forma $m \otimes n$ con $m \in M$ e $n \in N$ si dicono **tensori elementari** o **tensori monomiali**.*

Osservazione: Grazie al fatto che $m \otimes n = \tau(m,n)$ si hanno le seguenti proprietà per ogni $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ e $a \in A$:

1. $(m_1 + m_2) \otimes n = (m_1 \otimes n) + (m_2 \otimes n)$;
2. $m \otimes (n_1 + n_2) = (m \otimes n_1) + (m \otimes n_2)$;
3. $a(m \otimes n) = am \otimes n = m \otimes an$.

Proposizione 4.0.3 *Sia $M \otimes_A N$ prodotto tensoriale, valgono allora le seguenti proprietà:*

1. *$m \otimes 0 = 0 \otimes n = 0$ per ogni $m \in M, n \in N$;*
2. *L'insieme $L = \{m \otimes n |\ m \in M, n \in N\}$ è un insieme di generatori di $M \otimes N$;*
3. *Se $\mathcal{B}_M = \{m_1, ..., m_k\}$ è un insieme di generatori di M e $\mathcal{B}_N = \{n_1, ..., n_s\}$ è un insieme di generatori di N allora l'insieme $L = \{m \otimes n |\ m \in \mathcal{B}_M, n \in \mathcal{B}_N\}$ è un sistema di generatori di $M \otimes N$;*
4. *Se M, N sono finitamente generati, allora $M \otimes N$ è finitamente generato.*

Dimostrazione:

1. Conseguenza dell'osservazione precedente;
2. Dire che L genera $M \otimes N$ è equivalente a dire che $Q = (M \otimes N)/ < L >= 0$. Consideriamo il grafico:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi = 0} & Q \\ {\scriptstyle \tau}\downarrow & \nearrow_{\exists! \Phi} & \\ M \otimes N & & \end{array}$$

Sappiamo che $\Phi = 0$ fa commutare il diagramma, ma anche $\Phi = \pi$ proiezione al quoziente lo fa commutare: $\forall (m,n) \in M \times N$, $\pi(\tau(m,n)) = \pi(m \otimes n) = 0$. Per l'unicità di Φ si ha che $\pi = 0$ e cioè $Q = 0$;

3. Grazie al punto 2 sappiamo che i tensori elementari generano $M \otimes N$ ogni elemento può essere scritto come $(\sum_{i=1}^{k} a_i m_i \otimes \sum_{j=1}^{s} b_j n_j)$ grazie alle osservazioni fatte; questo ci da la tesi;

4. Conseguenza del punto 3.

$\bowtie$

ESEMPIO: $\mathbb{Z}/(a) \otimes_{\mathbb{Z}} \mathbb{Z}/(b) = 0$ con $(a, b) = 1$. Supponiamo senza perdita di generalità che $a < b$, allora un qualsiasi elemento $m \otimes n$ può essere scritto nella forma $m \otimes at = a(m \otimes t) = am \otimes t = 0 \otimes t = 0$. Tutti i tensori elementari sono dunque 0 e questo dimostra che $\mathbb{Z}/(a) \otimes_{\mathbb{Z}} \mathbb{Z}/(b) = 0$

ESEMPIO: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. Consideriamo il seguente diagramma:

$$\begin{array}{ccc} \mathbb{Q} \times \mathbb{Q} & \xrightarrow{\ b\ } & \mathbb{Q} \\ \Big\downarrow \tau & \nearrow \exists! \beta & \\ \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} & & \end{array}$$

con $b : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ forma bilineare tale che $b(x, y) = xy$. Esiste dunque $\beta : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$ tale che $\beta(x \otimes y) = xy$; vorremmo mostrare che β è un isomorfismo. Osserviamo che l'insieme $L = \{x \otimes 1 |\ x \in \mathbb{Q}\}$ è un sistema di generatori per $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$: consideriamo preliminarmente $x \otimes y = x \otimes \frac{a}{b} = \frac{xb}{b} \otimes \frac{a}{b} = \frac{x}{b} \otimes a = \frac{xa}{b} \otimes 1$ e dato che ogni tensore elementare lo posso scrivere come $x \otimes 1$ al variare di $x \in \mathbb{Q}$, l'insieme L genera $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$. Il morfismo β è chiaramente suriettivo; sia ora $m \otimes n = x \otimes 1 \in Ker\beta \Rightarrow \beta(x \otimes 1) = x = 0 \Rightarrow x = 0 \Rightarrow 0 = x \otimes 1 = m \otimes n$.

ESERCIZIO: Sia M uno $\mathbb{Z}$-modulo; caratterizzare $\mathbb{Q} \otimes_{\mathbb{Z}} M$. da fare

Proposizione 4.0.4 *Sia M A-modulo, allora $M \otimes_A A \cong M$.*

Dimostrazione: Consideriamo i morfismi

$$\begin{array}{rccc} \varphi : & M \otimes A & \longrightarrow & M \\ & m \otimes a & \longmapsto & am \end{array}$$

$$\begin{array}{rccc} \psi : & M & \longrightarrow & M \otimes A \\ & m & \longmapsto & m \otimes 1 \end{array}$$

Si verifica facilmente che $\psi = \varphi^{-1}$, cioè φ è un isomorfismo di A-moduli.

$\bowtie$

Definizione 4.5 *Dato M A-modulo si definisce **prodotto tensoriale multilineare** la struttura $M^{\otimes_n} = M \otimes ... \otimes M$*

Proposizione 4.0.5 *Dati M, N, P A-moduli, valgono le seguenti proprietà:*

1. $M \otimes N \cong N \otimes M$;
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$;
3. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$;
4. $(M \otimes A)/I(M \otimes A) \cong M/IM$.

Dimostrazione:

1. $\varphi : M \otimes N \to N \otimes M$ tale che $\varphi(m \otimes n) = n \otimes m$ è un isomorfismo di A-moduli: infatti il suo inverso è $\psi : N \otimes M \to M \otimes N$ tale che $\psi(n \otimes m) = m \otimes n$;
2. Mah!
3. Si verifica facilmente che $\varphi : (M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$ tale che $\varphi((m,n) \otimes p) = (m,p) \otimes (n,p)$ è un isomorfismo di A-moduli;
4. Conseguenza della proposizione precedente.

⋈

Proposizione 4.0.6 *Siano M, N A-moduli liberi; allora $M \otimes N$ è libero.*

Dimostrazione: Sia $M \cong A^m$ e $N \cong A^n$, allora $M \otimes N \cong A^m \otimes A^n \cong (A^{m-1} \oplus A) \otimes A^n \cong (A^{m-1} \otimes A^n) \oplus (A \otimes A^n) \cong (A^{m-1} \otimes A^n) \oplus A^n$. Ripetendo il medesimo passaggio m volte, si ottiene che $M \otimes N \cong A^{nm}$.

⋈

Notiamo che nella dimostrazione abbiamo anche dimostrato che $A^m \otimes_A A^n \cong A^{mn}$.

Abbiamo visto come è sempre possibile costruire il prodotto tensoriale tra due A-moduli; cerchiamo adesso di capire come si comporta il prodotto tensoriale rispetto ai morfismi: siano $f : M \to M'$ e $g : N \to N'$ morfismi di A moduli, consideriamo $M \otimes N$ e $M' \otimes N'$ e creiamo la seguente mappa:

$$\begin{array}{rccc} f \otimes g : & M \otimes N & \longrightarrow & M' \otimes N' \\ & m \otimes n & \longmapsto & f(m) \otimes g(n) \end{array}$$

Per verificarne la buona definizione usando la proprietà fondamentale basta mostrare che la mappa

$$\begin{array}{rccc} \varphi : & M \times N & \longrightarrow & M' \otimes N' \\ & (m,n) & \longmapsto & f(m) \otimes g(n) \end{array}$$

è bilineare cosicché abbiamo l'esistenza e l'unicità della mappa $f \otimes g$ che fa commutare il diagramma seguente:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & M' \otimes N' \\ {\scriptstyle\tau}\downarrow & \nearrow_{f \otimes g} & \\ M \otimes N & & \end{array}$$

Siano $m_1, m_2 \in M, n \in N$ allora $\varphi(m_1 + m_2, n) = f(m_1 + m_2) \otimes g(n) = (f(m_1) + f(m_2)) \otimes g(n) = (f(m_1) \otimes g(n)) + (f(m_2) \otimes g(n)) = \varphi(m_1, n) + \varphi(m_2, n)$. Inoltre sia $a \in A, m \in M, n \in N$ allora $\varphi(am, n) = f(am) \otimes g(n) = a(f(m) \otimes g(n)) = a\varphi(m, n)$. Le altre due verifiche sono analoghe.

Notiamo inoltre che l'operazione appena introdotta si comporta bene rispetto alla composizione, ovvero: siano f, g definite come sopra e $f' : M' \to M''$, $g' : N' \to N''$ altri due morfismi di A-moduli allora:

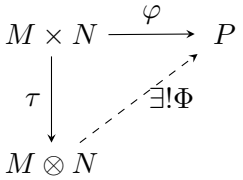
$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

Come conseguenza delle osservazioni fatte, dato un $A-$modulo M, possiamo considerare $\cdot \otimes M = M \otimes \cdot$ come un funtore covariante della categoria degli $A-$moduli in sé. In particolare, il funtore agisce nel seguente modo:

$$\begin{array}{rccc} \cdot \otimes M : & \text{A-moduli} & \longrightarrow & \text{A-moduli} \\ & N & \longmapsto & N \otimes M \\ & f : N \to P & \longmapsto & f \otimes id_M : N \otimes M \to P \otimes M \end{array}$$

Lemma 4.0.7 *Siano M, N, P A-moduli, allora $Hom(M \otimes N, P) \cong Hom(M, Hom(N, P)) \cong Bil(M, N, P)$.*

Dimostrazione: L'ultimo isomorfismo è già stato dimostrato. Ci basta dunque mostrare che $Hom(M \otimes N, P) \cong Bil(M, N, P)$ Consideriamo la proprietà universale del prodotto tensore valida $\forall \varphi \in Bil(M, N, P)$:



Definiamo dunque il morfismo $f : Hom(M \otimes N, P) \to Bil(M, N, P)$ tale che $f(\varphi) = \Phi$. Le verifiche che f sia un isomorfismo discendono direttamente dalla proprietà universale.

⋈

Proposizione 4.0.8 *Per ogni M, N, P A-moduli, sono fatti equivalenti:*

1. *$M \xrightarrow{f} N \xrightarrow{g} P \to 0$ è esatta;*
2. *$\forall Q$ A-modulo, $M \otimes Q \xrightarrow{f \otimes id_Q} N \otimes Q \xrightarrow{g \otimes id_Q} P \otimes Q \longrightarrow 0$ è esatta.*

Dimostrazione:

$1 \Rightarrow 2$) Grazie alla caratterizzazione del funtore $Hom(\star, L)$ possiamo riscrivere l'ipotesi come $0 \to Hom(P, L) \to Hom(N, L) \to Hom(M, L)$ è esatta per ogni L, e la tesi come:

$$0 \to Hom(P \otimes Q, T) \to Hom(N \otimes Q, T) \to Hom(M \otimes Q, T)$$

è esatta $\forall T$. Sfruttando il lemma precedente, la tesi equivale nuovamente a:

$$0 \to Hom(P, Hom(Q, T)) \to Hom(N, Hom(Q, T)) \to Hom(M, Hom(Q, T))$$

è esatta $\forall Q$. Ma questo segue dalla seconda formulazione dell'ipotesi poiché basta porre $L = Hom(Q, T)$;

$2 \Rightarrow 1$) Basta porre $Q = A$ e si ha la tesi.

⋈

In generale, il funtore $\cdot \otimes M$ non conserva l'iniettività e dunque non è esatto. Questo ci porta a dare una particolare importanza alla seguente famiglia di moduli:

Definizione 4.6 *Un $A-$modulo Q per cui $\otimes Q$ trasforma successioni esatte corte in successioni esatte corte si dice* ***modulo piatto****.*

Osservazione: Notiamo il seguente fatto che ci sarà utile per la prossima dimostrazione: siano Q_1, Q_2, T_1, T_2 $A-$moduli. Allora:

$$\begin{array}{l} 0 \to Q_1 \xrightarrow{q} Q_2 \\ \qquad\qquad \text{q, t iniettive} \iff 0 \to Q_1 \oplus T_1 \xrightarrow{(q,t)} Q_2 \oplus T_2 \quad \text{(q, t) iniettiva} \\ 0 \to T_1 \xrightarrow{t} T_2 \end{array}$$

Proposizione 4.0.9 *Siano N_1, N_2 $A-$moduli. Allora:*

1. *N_1, N_2 proiettivi $\Rightarrow N_1 \otimes N_2$ è proiettivo;*

2. *N_1 e N_2 piatti $\Rightarrow N_1 \otimes N_2$ è piatto ;*

3. *N_1, N_2 piatti $\Leftrightarrow N_1 \oplus N_2$ è piatto.*

Dimostrazione:

1. Supponiamo che N_1 e N_2 siano proiettivi. Allora esistono due coppie di $A-$moduli G_1, F_1 e G_2, F_2 con gli F_i liberi tali che $F_1 = N_1 \oplus G_1$ e $F_2 = N_2 \oplus G_2$. Allora:

$$F_1 \otimes F_2 = (N_1 \oplus G_1) \otimes (N_2 \oplus G_2) = (N_1 \otimes N_2) \oplus (N_1 \otimes G_2) \oplus (G_1 \otimes N_2) \oplus (G_1 \otimes G_2)$$

   E poiché $F_1 \otimes F_2$ è libero, $N_1 \otimes N_2$ è proiettivo perché addendo diretto di un modulo libero.

2. Semplice verifica.

3. $\Leftarrow$) Se $N_1 \oplus N_2$ è piatto e si ha la successione esatta $0 \to M \xrightarrow{f} N$, allora $0 \to M \otimes (N_1 \oplus N_2) \to N \otimes (N_1 \oplus N_2)$ è esatta. Ma $M \otimes (N_1 \oplus N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$ e $N \otimes (N_1 \oplus N_2) \cong (N \otimes N_1) \oplus (N \otimes N_2)$. Per l'osservazione fatta, si hanno le successioni esatte:

$$0 \to M \otimes N_1 \to N \otimes N_1$$

$$0 \to M \otimes N_2 \to N \otimes N_2$$

   e quindi N_1 e N_2 sono piatti.

4. $\Rightarrow$) Si ripercorre la precedente dimostrazione a ritroso.

$\bowtie$

Forniamo adesso un controesempio alle implicazioni inverse di $1, 2$ della proposizione precedente: $0 = \mathbb{Z}/(5) \otimes_{\mathbb{Z}} \mathbb{Z}/(7)$ è proiettivo ma, $\mathbb{Z}/(5)$ non è proiettivo (non è addendo diretto di $\mathbb{Z}/(25)$ di cui è quoziente).
Notiamo inoltre che 0 è piatto ma $\mathbb{Z}/(5)$ non lo è. Infatti, considerando la successione esatta $0 \to \mathbb{Z} \xrightarrow{\cdot 5} \mathbb{Z}$, tensorizzando rispetto a $\mathbb{Z}$ con $\mathbb{Z}/(5)$ l'applicazione $\cdot 5$ diventa l'applicazione nulla, e dunque la successione tensorizzata $0 \to \mathbb{Z}/(5) \xrightarrow{(\cdot 5)\otimes id_{\mathbb{Z}}} \mathbb{Z}/(5)$ non è esatta.

Mettiamo ora in evidenza due importanti operazioni che si possono compiere con i moduli, ovvero poter definire su un A-modulo M una struttura di B-modulo grazie a un morfismo di anelli tra A e B:

Restrizione di scalari: Siano A, B anelli, $f : A \to B$ un morfismo di anelli e M un B-modulo. Possiamo far si che M sia anche un A-modulo mediante il seguente prodotto esterno: sia $a \in A$ e $m \in M$, allora $a \cdot m = f(a)m$. In questo modo l'operazione è ben definita (sto moltiplicando un elemento di B per M);

Estensione di scalari: Siano A, B anelli, $f : A \to B$ un morfismo di anelli e N un A-modulo. Come sopra, lo scopo è quello di dare a N una struttura di B-modulo, ma ci sono dei problemi al riguardo; riusciamo però a definire una struttura di B-modulo al prodotto tensoriale $N \otimes_A B$ (che sappiamo essere ben definito poiché possiamo vedere B come un A-modulo per la restrizione). Definiamo dunque il prodotto esterno per ogni $b \in B$ e per ogni $(n \otimes_A \tilde{b}) \in N \otimes_A B$ come $b \cdot (n \otimes_A \tilde{b}) = n \otimes_A b\tilde{b}$.

Lemma 4.0.10 *Siano A e B anelli, M un $A-$modulo, P un B-modulo e N con struttura doppia di A-modulo e B-modulo. Allora $M \otimes_A (N \otimes_B P) \cong (M \otimes_A N) \otimes_B P$.*

Dimostrazione: Definiamo le due mappe:

$$\begin{array}{rccc} \varphi: & M \otimes_A (N \otimes_B P) & \longrightarrow & (M \otimes_A N) \otimes_B P \\ & m \otimes_A (n \otimes_B p) & \longmapsto & (m \otimes_A n) \otimes_B p \end{array}$$

$$\begin{array}{rccc} \psi: & (M \otimes_A N) \otimes_B P & \longrightarrow & M \otimes_A (N \otimes_B P) \\ & (m \otimes_A n) \otimes_B p & \longmapsto & m \otimes_A (n \otimes_B p) \end{array}$$

La buona definizione dei morfismi deriva dalla proprietà universale del prodotto tensoriale e le mappe sono evidentemente una l'inversa dell'altra.

⋈

Lemma 4.0.11 *Sia A anello e I un ideale di A e M un A-modulo, allora $A/I \otimes_A M \cong M/IM$.*

Dimostrazione: Consideriamo la successione esatta di A-moduli $0 \to I \xrightarrow{i} A \xrightarrow{\pi} A/I \to 0$ e applichiamo il funtore $\cdot \otimes M$ ottenendo la successione esatta

$$I \otimes M \xrightarrow{i\otimes id = f} A \otimes M \xrightarrow{\pi \otimes id = g} A/I \otimes M \to 0$$

Per capire chi è $A/I \otimes M$ ci basta studiare il quoziente $(A \otimes M)/(Kerg) \cong (A \otimes M)/Imf$. Sappiamo che $A \otimes M \cong M$ tramite il morfismo φ tale che $\varphi(a \otimes m) = am$. Cerchiamo allora di capire chi è $M/Im\tilde{f} \cong (A \otimes M)/Imf$ con $\tilde{f} = \varphi \circ f$, ovvero $\tilde{f} : I \otimes M \to M$ è tale che $\tilde{f}(i \otimes m) = im$. Mostriamo che $Im\tilde{f} = IM$: sia $x \in Im\tilde{f} \Rightarrow x = im$ per un certo $i \in I, m \in M$. Viceversa sia $im \in IM \Rightarrow \tilde{f}(i \otimes m) = im$. Dunque $IM = im\tilde{f}$ e $A/I \otimes_A M \cong M/IM$.

⋈

Definizione 4.7 *Sia (A, I) anello locale, $\mathbb{K} = A/I$, M A-modulo finitamente generato; definiamo $\mu(M) = dim_{\mathbb{K}}(M \otimes_A \mathbb{K}) = dim_{\mathbb{K}}(M/IM)$.*

Notiamo che la definizione è ben posta poiché M/IM è un A/I modulo e cioè un $\mathbb{K}$ spazio vettoriale. Inoltre $\mu(M)$ è finita poiché M è finitamente generato.

Proposizione 4.0.12 *Sia (A, I) un anello locale, $\mathbb{K} = A/I$, M, N $A-$moduli finitamente generati non nulli. Allora $\mu(M \otimes_A N) = \mu(M)\mu(N)$*

Dimostrazione: $\mu(M \otimes_A N) = dim_{\mathbb{K}}(M \otimes_A N \otimes_A \mathbb{K})$, ma:

$$M \otimes_A N \otimes_A \mathbb{K} \cong M \otimes_A (\mathbb{K} \otimes_A N) \cong M \otimes_A ((\mathbb{K} \otimes_{\mathbb{K}} \mathbb{K}) \otimes_A N) \cong M \otimes_A (\mathbb{K} \otimes_{\mathbb{K}} (\mathbb{K} \otimes_A N))$$

che, per il lemma, è isomorfo a

$$(M \otimes_A \mathbb{K}) \otimes_{\mathbb{K}} (\mathbb{K} \otimes_A N) \cong \mathbb{K}^{\mu(M)} \otimes_{\mathbb{K}} \mathbb{K}^{\mu(N)} \cong \mathbb{K}^{\mu(M)\mu(N)}$$

da cui la tesi.

⋈

Proposizione 4.0.13 *Sia (A, I) un anello locale, $\mathbb{K} = A/I$ e M un A-modulo finitamente generato. Allora M è libero $\iff$ M è proiettivo.*

Dimostrazione: Abbiamo già dimostrato che in generale libero implica proiettivo. Mostriamo il viceversa sotto le opportune ipotesi. Poiché M è finitamente generato, esiste $n \in \mathbb{N}$ tale che la successione $A^n \to M \xrightarrow{f} 0$ è esatta. Ora, A è un anello locale, quindi possiamo porre

$n = dim_{\mathbb{K}}(M/IM)$. Si ha dunque la successione esatta $0 \to Kerf \to A^n \xrightarrow{f} M \to 0$, da cui $A^n = M \oplus Kerf$ per proiettività di M. Tensorizzando entrambi i membri per $\mathbb{K}$, si ottiene

$$A^n \otimes_A \mathbb{K} \cong A^n \otimes_A A/I \cong A^n/IA^n \cong \mathbb{K}^n$$

$$(M \otimes_A \mathbb{K}) \oplus (Kerf \otimes_A \mathbb{K}) \cong (M \otimes_A A/I) \oplus (Kerf \otimes_A A/I) \cong Kerf/IKerf \oplus M/IM$$

da cui, per questioni dimensionali, $Kerf/IKerf = 0 \Rightarrow Kerf = IKerf$ e dunque, per il Lemma di Nakayama, $Kerf = 0$ e $A^n \cong M$.

⋈

Capitolo 5

Decomposizione primaria e anelli notheriani

Definizione 5.1 *Un ideale $Q \subseteq A$ si dice P-primario se è primario e $\sqrt{Q} = P$.*

Proposizione 5.0.1 *Sia $Q \subseteq A$ un ideale $P-$primario. Allora:*

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

Dimostrazione:

1. Vale in generale $(1 \in (Q : x))$.
2. Sia $a \in (Q : x) \Rightarrow ax \in Q$. Ma $x \notin Q$ per ipotesi, quindi $a^n \in Q$ per qualche $n \in \mathbb{N}$, ossia $a \in P$, da cui $Q \subseteq (Q : x) \subseteq P$. Passando al radicale, si ottiene: $P = \sqrt{Q} \subseteq \sqrt{(Q : x)} \subseteq \sqrt{P} = P \Rightarrow \sqrt{(Q : x)} = P$. Adesso mostriamo che $(Q : x)$ è primario. Sia $ab \in (Q : x)$ e supponiamo $b \notin P$, (ossia $b^n \notin (Q : x)$ per nessun $n \in \mathbb{N}$): vogliamo mostrare che $a \in (Q : x)$. Per ipotesi $abx \in Q$, ma $b^n \notin Q$, quindi $ax \in Q$ per primarietà e dunque $a \in (Q : x)$.
3. Sia $a \in (Q : x) \Rightarrow ax \in Q$, ma per ipotesi $x \notin P$, ossia $x^n \notin Q$, quindi $a \in Q$. Allora $(Q : x) \subseteq Q$. L'altra inclusione è vera in generale, dunque $(Q : x) = Q$.

⋈

Definizione 5.2 *Un ideale $I \subseteq A$ si dice* ***decomponibile*** *se può essere espresso come intersezione finita di ideali primari.*
Data la decomposizione $I = \bigcap_{i=1}^{n} Q_i$ con Q_i primario $\forall\, i$, ponendo $P_i = \sqrt{Q_i}$, la decomposizione si dice ***minimale*** *(o irridondante) se*

- $P_i \neq P_j \; \forall i \neq j$;
- $\forall\, i \; Q_i \not\supseteq \bigcap_{i \neq j} Q_j$

Osserviamo che, data una decomposizione in primari di un ideale I, è sempre possibile fare in modo che la seconda condizione sia soddisfatta (è sufficiente eliminare gli ideali che contengono l'intersezione degli altri). La prossima proposizione mostra che ci si può ridurre anche alla prima condizione.

Proposizione 5.0.2 *Sia $I = Q_1 \cap Q_2$ con $Q_1,\ Q_2$ ideali $P-$primari. Allora anche I è $P-$primario.*

Dimostrazione: Sia $xy \in I$ e supponiamo che $x \notin Q_1 \ \Rightarrow\ y^n \in Q_1 \ \Rightarrow\ y \in \sqrt{Q_1} = P = \sqrt{Q_2}$, ossia $y^m \in Q_2$. Ma allora $y^{n+m} \in I$ e quindi I è primario. Inoltre $\sqrt{I} = \sqrt{Q_1} \cap \sqrt{Q_2} = P$, da cui I è $P-$primario.

$\bowtie$

Teorema 5.0.3 *Sia $I = \bigcap_{i=1}^n Q_i$ decomposizione minimale in primari e poniamo $P_i = \sqrt{Q_i}\ \forall\ i$. Allora $\{P_i | i = 1, \dots, n\} = \{\text{ideali primi di } \Sigma\}$ dove $\Sigma = \{\sqrt{(I : a)} | a \in A\}$.*

Dimostrazione: Osserviamo che $(I : a) = (\bigcap_i Q_i : a) = \bigcap_i (Q_i : a)$; mostriamo ora le due inclusioni:

$\supseteq$) Innanzitutto, se a appartiene all'intersezione di tutti i Q_i, $(I : a) = A$, che non è primo; in caso contrario $\sqrt{(I : a)} = \bigcap_i \sqrt{(Q_i : a)} = \bigcap_{a \notin Q_i} P_i$ per la proposizione 5.0.1. Ma se $\sqrt{(I : a)}$ è primo allora per un qualche j, $\sqrt{(I : a)} = P_j$ grazie alla proposizione 1.1.9.

$\subseteq$) Poiché la decomposizione è minimale sappiamo che per ogni i esiste $a_i \notin Q_i$ tale che $a_i \in \bigcap_{j \neq i} Q_j$. Allora $\sqrt{(I : a_i)} = \bigcap_j \sqrt{(Q_j : a_i)} = \bigcap_{j \neq i} \sqrt{(Q_j : a_i)} \cap \sqrt{(Q_i : a_i)} = P_i$ applicando il primo e secondo punto della proposizione 5.0.1.

$\bowtie$

Definizione 5.3 *Con le notazioni del teorema precedente, i P_i si dicono **primi associati**. Gli elementi minimali si dicono **primi minimali** e gli altri sono detti **primi immersi**.*

Osservazione: Dal teorema dimostrato segue che i P_i dipendono soltanto da I e non dalla decomposizione scelta. Inoltre osserviamo che i primi minimali sono anche gli elementi minimali nell'insieme dei primi che contengono I: infatti $P \supseteq I = \bigcap_i Q_i \ \Rightarrow\ P \subseteq \sqrt{I} = \bigcap_i P_i$ dove i P_i sono minimali, quindi $P \supseteq P_j$ per un qualche j.

Proposizione 5.0.4 *Sia A un anello tale che l'ideale (0) è decomponibile, cioè $(0) = \bigcap_i Q_i$ e $\sqrt{Q_i} = P_i$. Allora:*

1. *$\mathcal{D}(A) = \bigcup_i P_i$ primi associati.*
2. *$\mathcal{N}(A) = \bigcap_i P_i$ primi minimali.*

Dimostrazione: Come abbiamo visto ad esercitazione, $\mathcal{D}(A) = \bigcup_{a \neq 0} \sqrt{(0 : a)} \supseteq \bigcup_i P_i$ per quanto visto. D'altra parte, poiché $a \neq 0$, a non appartiene all'intersezione dei Q_i, e dunque $\sqrt{(0 : a)} = \bigcap_i \sqrt{(Q_i : a)} = \bigcap_{a \notin Q_i} P_i \subseteq P_j$ per un certo j, e questo dimostra la seconda inclusione.
Il secondo punto è una banale conseguenza dell'osservazione precedente, ricordando che $\mathcal{N}(A) = \bigcap_{P \text{primo}} P = \bigcap_{P \supseteq (0)} P$.

$\bowtie$

Esercizio: Sia $A = \mathbb{K}[x, y, z, t]$ e si consideri l'ideale $I = (x^2z - x^2t^3, x^2y^4t + x^2y^3 - x^2z, xt^2)$. Scrivere una decomposizione primaria irridondante di I e dire quali sono i primi associati e quali i primi minimali. Trovare $\mathcal{N}(A/I)$ e $\mathcal{D}(A/I)$.
Svolgimento: Innanzitutto troviamo una base di Groebner per I: $I = (x^2z, xt^2, x^2y^4t + x^2y^3)$ e fissiamo l'ordinamento *Lex* $x > y > z > t$.
$S(f_1, f_3) = zf_3 - y^4tf_1 = x^2y^3z \xrightarrow{f_1} 0$
$S(f_2, f_3) = tf_3 - xy^4f_2 = x^2y^3t = f_4$
Quindi $I = (x^2z, xt^2, x^2y^3)$ è monomiale. Usando la solita proprietà degli ideali monomiali

$$(x^2z, xt^2, x^2y^3) = (x) \cap (t^2, x^2z, x^2y^3) = (x) \cap (t^2, x^2) \cap (t^2, z, x^2y^3) =$$

$$= (x) \cap (t^2, x^2) \cap (t^2, x^2, z) \cap (y^3, t^2, z) = (x) \cap (t^2, x^2) \cap (y^3, t^2, z)$$

è una decomposizione primaria per la caratterizzazione degli ideali monomiali primari. I primi associati sono $(x), (x, t)$ e (y, z, t), con (x), (y, z, t) minimali. La decomposizione è irridondante perché i primi associati sono tutti distinti e nessuno dei tre ideali contiene l'intersezione degli altri due.
Ora, l'ideale (0) dell'anello quoziente A/I può essere espresso come $((x) \cap (t^2, x^2) \cap (y^3, t^2, z))A/I$ e dunque è decomponibile. Applicando la precedente proposizione

$$\mathcal{N}(A/I) = ((x) \cap (y, z, t))A/I = (xy, xz, xt)A/I$$

$$\mathcal{D}(A/I) = ((x) \cup (x, t) \cup (y, z, t))A/I = ((x, t) \cup (y, z, t))A/I$$

Proposizione 5.0.5 *Siano $Q \subseteq A$ un ideale $P-$primario e $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso. Se $S \cap P \neq \emptyset$ allora $S^{-1}Q = S^{-1}A$; invece se $S \cap P = \emptyset$, allora $S^{-1}Q$ è $S^{-1}P-$primario e $(S^{-1}Q)^c = Q$.*

Dimostrazione: Se $s \in S \cap P \Rightarrow s^n \in S \cap Q$, e quindi $S^{-1}Q = S^{-1}A$.
Supponendo invece che $S \cap P = \emptyset$, si ha $\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$. Sia ora $\frac{a}{s}\frac{b}{t} \in S^{-1}Q$ e supponiamo $\frac{a}{s} \notin S^{-1}P$. Allora $\frac{ab}{st} = \frac{q}{r}$ con $q \in Q$ e $r \in S$, ossia $\exists\ u \in S$ tale che $uabr = uqst$. Ora, $uqst \in Q$ e dunque $urab \in Q$, ma $ur \notin P \Rightarrow ab \in Q \Rightarrow b \in Q$, in quanto per ipotesi $a \notin P$. Di conseguenza $S^{-1}Q$ è $S^{-1}P-$primario.
Per l'ultima parte, in generale vale che $Q \subseteq Q^{ec} = (S^{-1}Q)^c$. Mostriamo l'altra inclusione: sia $a \in (S^{-1}Q)^c$, allora $\frac{a}{1} \in S^{-1}Q$, ossia $\frac{a}{1} = \frac{b}{s}$ con $b \in Q$. Deve quindi esistere $u \in S$ tale che $uas = ub \Rightarrow usa \in Q$. Ma $us \notin P \Rightarrow a \in Q$, come volevamo mostrare.

⋈

Esercizio: Siano $S \subseteq A$ un sottoinsieme moltiplicativo, $I = \bigcap_i Q_i$ una decomposizione minimale in primari. Calcolare una decomposizione di $S^{-1}I$ e $(S^{-1}I)^c$
Svolgimento: Osserviamo innanzitutto che:

$$S^{-1}I = \bigcap_{P_i \cap S = \emptyset} S^{-1}Q_i \overset{wlog}{=} S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_m$$

è una decomposizione minale di $S^{-1}I$, infatti:

- I primi associati sono $S^{-1}P_1, \ldots, S^{-1}P_m$ (dove per ogni i $P_i \cap S = \emptyset$), in corrispondenza biunivoca con i P_i e quindi tutti distinti.
- Supponiamo per assurdo che esista un indice i per cui $S^{-1}Q_i \supseteq \bigcap_{j \neq i} S^{-1}Q_j$. Allora passando al contratto e applicando la proposizione precedente, si ha:

$$Q_i = (S^{-1}Q_i)^c \supseteq (\bigcap_{j \neq i} S^{-1}Q_j)^c = \bigcap_{j \neq i} (S^{-1}Q_j)^c = \bigcap_{j \neq i} Q_j$$

  assurdo, perché la decomposizione di I nei Q_i è minimale.

Con gli stessi passaggi segue inoltre che $(S^{-1}I)^c = \bigcap_{P_i \cap S = \emptyset} Q_i$.

Definizione 5.4 *Sia $(\Sigma, \leq)$ un insieme con un ordinamento parziale. Una catena $C \subseteq \Sigma$ si dice **ascendente** se i suoi elementi sono indicizzati da $\mathbb{N}$ in modo tale che $\forall\ i \in \mathbb{N}$, $c_i \leq c_{i+1}$ e non esiste $d \in C$ tale che $c_i < d < c_{i+1}$*

Proposizione 5.0.6 *Sia $(\Sigma, \leq)$ un insieme con un ordinamento parziale. Sono fatti equivalenti:*

1. *Ogni sottoinsieme $P \subseteq \Sigma$, $P \neq \emptyset$ ammette un elemento massimale (*Maximal Condition*);*

2. *Ogni catena ascendente $s_1 \leq s_2 \leq \dots$ si stabilizza in un numero finito di passi, cioè $\exists N \in \mathbb{N}$ tale che $\forall m > N$ $s_m = s_N$ (*Ascending Chain Condition*)*

Dimostrazione:

$1 \Rightarrow 2)$ Sia $S = \{s_1 \leq s_2 \leq \dots\}$ una catena ascendente in Σ. Essendo $S \neq \emptyset$, per ipotesi S ammette un elemento massimale $s_N \in S$. Segue la tesi.

$2 \Rightarrow 1)$ Supponiamo per assurdo che esista un sottoinsieme non vuoto $P \subseteq \Sigma$ che non ammetta elementi massimali. Allora $\forall\ s_i \in P\ \exists s_{i+1} > s_i$, quindi utilizzando l'Assioma della Scelta possiamo costruire una catena ascendente $s_1 < s_2 < \dots$ infinita, assurdo.

$\bowtie$

Definizione 5.5 *Un anello si dice **Noetheriano** se l'insieme dei suoi ideali soddisfa l' Ascending Chain Condition. Un $A-$ modulo si dice **Noetheriano** se l'insieme dei suoi sottomoduli soddisfa l' ACC.*

Definizione 5.6 *Dato un insieme Σ non vuoto, diremo che Σ soddisfa la **Descending Chain Condition** se ogni catena discendente $s_1 \geq s_2 \geq \dots$ si stabilizza in un numero finito di passi.*

Definizione 5.7 *Un anello si dice **Artiniano** se l'insieme dei suoi ideali soddisfa la Descending Chain Condition. Un $A-$ modulo si dice **Artiniano** se l'insieme dei suoi sottomoduli soddisfa la DCC.*

Esempi:

- $\mathbb{K}[x_1, \dots, x_n]$ è noetheriano ma non artiniano.
- $\mathbb{Z}$ è noetheriano ma non artiniano:$(p) \supsetneq (p^2) \supsetneq \dots$
- $\mathbb{K}$ come campo è sia noetheriano che artiniano.
- Se un anello A è noetheriano, allora (per il teorema della base di Hilbert) anche $A[x]$ è noetheriano (e per induzione $A[x_1, \dots, x_n]$).

Proposizione 5.0.7 *Un $A-$modulo M è noetheriano $\iff$ ogni suo sottomodulo è finitamente generato.*

Dimostrazione:

$\Rightarrow$) Sia M noetheriano e consideriamo $N \subseteq M$ un suo sottomodulo. Costruiamo l'insieme $\Sigma = \{$sottomoduli di N finitamente generati$\}$. Sicuramente $\Sigma \neq \emptyset$ perché $0 \in \Sigma$, quindi per la Proposizione 5.0.6 esiste un elemento massimale N_0 in Σ (e dunque N_0 finitamente generato). Se $N_0 = N$ abbiamo finito; altrimenti, dovrà esistere un elemento $n \in N - N_0$, da cui $N \supseteq N_0 + \langle n \rangle \supsetneq N_0$ risulterebbe finitamente generato, assurdo.

$\Leftarrow$) Consideriamo una catena ascendente di sottomoduli $M_1 \subseteq M_2 \subseteq \dots$. Poiché i moduli sono contenuti l'uno nell'altro, anche $N = \bigcup_i M_i$ è un sottomodulo di M, e quindi $N = \langle m_1, \dots, m_k \rangle \Rightarrow \exists \overline{k}$ tale che $M_{\overline{k}} \supseteq \langle m_1, \dots, m_k \rangle$, da cui la catena si stabilizza.

⋈

OSSERVAZIONE: Grazie a quanto dimostrato è evidente che ogni sottomodulo di un $A-$modulo Noetheriano è Noetehriano.

Enunciamo ora un importante risultato, senza però riportarne la dimostrazione:

Teorema 5.0.8 *Sia* $0 \to M_1 \to M \to M_2 \to 0$ *una successione esatta di* $A-$*moduli. Allora* M *è noetheriano (artiniano) se e solo se* M_1 *e* M_2 *sono noetheriani (artiniani).*

Corollario 5.0.9 *Valgono le seguenti proprietà:*

1. $\bigoplus_1^n M_i$ *con* M_i *noetheriani è noetheriano.*
2. A *noetheriano,* $I \subseteq A$ *ideale* $\Rightarrow$ A/I *noetheriano.*
3. A *noetheriano,* M $A-$*modulo finitamente generato* $\Rightarrow$ M *noetheriano.*

Dimostrazione: Conseguenze immediate del teorema precedente

⋈

Teorema 5.0.10 *Sia* A *un anello Noetheriano, allora qualsiasi ideale* $I \subseteq A$ *è decomponibile.*

Dimostrazione: Innanzitutto dimostriamo che ogni ideale di A può essere espresso come intersezione finita di ideali irriducibili, e poi mostreremo che ogni ideale irriducibile è primario.

1. Supponiamo per assurdo che esista un ideale che non può essere espresso come intersezione finita di ideali irriducibili, allora l'insieme

   $$\Sigma = \{\text{ideali di A che non sono intersezione finita di irriducibili}\}$$

   è un sottoinsieme non vuoto di {ideali di A} e dunque per l'equivalenza di ACC e MC (Proposizione 5.0.6) ammette elemento massimale J. J non è irriducibile per ipotesi e dunque devono esistere ideali $J_1 \supsetneq J$, $J_2 \supsetneq J$ tali che $J_1 \cap J_2 = J$. Per l'ipotesi di massimalità J_1 e J_2 sono intersezione di irriducibili e così è J, assurdo.

2. Consideriamo l'anello quoziente A/I (che sappiamo essere Noetheriano) e dimostriamo (0) irriducibile $\Rightarrow$ (0) primario: sia $ab = 0$ con $b \neq 0$, vogliamo mostrare che $a^n = 0$. $0 \neq Ann(a) \subseteq Ann(a^2) \subseteq \cdots \subseteq Ann(a^n) = Ann(a^{n+1})$ per Noetherianità. Se dimostriamo che $(a^n) \cap (b) = (0)$, allora per irriducibilità di (0) e per l'ipotesi $(b) \neq (0)$ $(a^n) = (0)$, che è la tesi.
   Ovviamente $(a^n) \cap (b) \supseteq (0)$. Sia ora c un elemento dell'intersezione: $c = ka^n = hb\ ka^{n+1} = h(ab) = 0$, quindi $k \in Ann(a^{n+1}) = Ann(a^n) \Rightarrow c = ka^n = 0$. In conclusione $(a^n) \cap (b) = (0)$, che è quello che volevamo dimostrare.

⋈

Proposizione 5.0.11 *Sia* A *un anello e* $S \subseteq A$ *un sottoinsieme moltiplicativamente chiuso. Se* A *è Noetheriano, allora* $S^{-1}A$ *è Noetheriano.*

Dimostrazione: Sappiamo che gli ideali di $S^{-1}A$ sono tutte e sole le estensioni di ideali di A. Sia dunque $J \subseteq S^{-1}A$ un ideale e $I \subseteq A$ tale che $J = I^e = S^{-1}I$, con $I = (f_1, \ldots, f_k)$: per definizione $I^e = (\frac{f_1}{1}, \ldots, \frac{f_k}{1})$ è finitamente generato e dunque $S^{-1}A$ è Noetheriano.

⋈

Esercizio: Sia A anello Artiniano locale con I ideale massimale, cosa possiamo dire su $S^{-1}A$ con S moltiplicativamente chiuso? *Svolgimento:* Per quanto riguarda la seconda parte, dimostriamo preliminarmente che un anello Artiniano A (possibilmente non locale) è unione disgiunta delle sue unità e dei suoi zero-divisori, ossia $A = A^* \cup \mathcal{D}(A)$. Infatti se $a \notin A^*$, ho la catena discendente $(a) \supsetneq (a^2) \supsetneq \cdots \supsetneq (a^k) = (a^{k+1})$, da cui esiste $\alpha \in A$ tale che $a^k = \alpha a^{k+1} \Rightarrow a^k(1 - \alpha a) = 0$. Poiché $1 - \alpha a \neq 0$ (altrimenti a sarebbe un'unità), a^k è uno zero divisore, e quindi (per induzione) anche a è uno zero divisore.
Se ora A è anche locale, si ha $A = A^* \cup I$. Abbiamo due casi:

- Se $S \cap I \neq \emptyset$, allora $S^{-1}I = S^{-1}A$.
- Se $S \cap I = \emptyset$, allora $S \subseteq A - I = A^*$ e dunque sto invertendo elementi che erano già unità, ossia $S^{-1}A \cong A$ (per essere rigorosi dovremmo applicare la proprietà universale a id_A).