Algebra II

Alessandra Tullini

2016/2017

Indice

Questi appunti sono frutto della rielaborazione delle lezioni di Algebra II tenute durante l'anno accademico 2016/2017 dalla Prof.ssa Gianni e dal Prof. Sbarra. Non escludo la possibilità che vi siano degli errori, motivo per cui vi chiedo di scusarmi e vi invito a contattarmi all'indirizzo `tullini[at]mail.dm.unipi.it` per segnalarmeli.

Se non avete seguito il corso di Algebra II, è probabile che talvolta vi troviate spaesati. Il motivo sta nel fatto che non ho (ancora) trovato il tempo di trascrivere svariati dettagli.

Capitolo 1

Risultati Preliminari

Per prima cosa dimostreremo alcuni risultati propedeutici sugli ideali di A anello commutativo con unità. Non ripeteremo le definizioni di somma, prodotto, intersezione, colon e radicale, ma sarà utile ricordare che se I, J, H sono ideali di A, allora $(I+J)(I\cap J) = IJ$ e $I\cap(J+H) = (I\cap J)+(I\cap H)$, da cui la *legge modulare*: se $I \subseteq H$, allora $(I+J)\cap H = I + J\cap H$.

Definizione 1.0.1 (Radicale di Jacobson)**.** *Sia A anello con unità e $\mathfrak{m}$ un suo generico ideale massimale. Definiamo Radicale di Jacobson di A l'ideale*

$$\mathfrak{J}(A) = \bigcap_{\mathfrak{m}\subseteq A} \mathfrak{m}.$$

Proposizione 1.0.1 (Caratterizzazione del Radicale di Jacobson)**.** *$\forall x \in A$ si ha che $x \in \mathfrak{J}(A) \Leftrightarrow \forall y \in A\ 1-xy \in A^*$*

Dimostrazione. ($\Leftarrow$) Dimostriamo la contronominale: sia $x \notin \mathfrak{J}(A) \Leftrightarrow \exists \mathfrak{m} \mid x \notin \mathfrak{m} \Rightarrow \mathfrak{m} \subsetneq (\mathfrak{m}, x)$. Per massimalità, $(\mathfrak{m}, x) = A = (1)$, da cui $1 = m + xy, ,\ m \in \mathfrak{m},\ y \in A \Leftrightarrow 1 - xy = m \in \mathfrak{m} \Rightarrow 1-xy$ non può essere invertibile.
($\Rightarrow$) Supponiamo che $\exists y \in A \mid 1-xy \notin A^* \Rightarrow \exists \mathfrak{m} \mid 1-xy \in \mathfrak{m} \Leftrightarrow 1-xy = m,\ m \in \mathfrak{m} \Leftrightarrow 1 = m + xy \Rightarrow xy \notin \mathfrak{m} \Rightarrow x \notin \mathfrak{J}(A)$ □

Proposizione 1.0.2 (Comassimalità, Prodotto e Intersezione)**.** *$I, J \subseteq A$ ideali. $I + J = (1) \Rightarrow I \cap J = IJ$.*

Dimostrazione. In generale $IJ \subseteq I \cap J$. Se però $I + J = (1) \Rightarrow 1 = i + j,\ i \in I,\ j \in J$. Preso dunque $\alpha \in I \cap J \Rightarrow \alpha = 1\alpha = i\alpha + j\alpha \in IJ$. □

Lemma 1.0.1. *Sia P un ideale primo, e siano $I_1, \cdots, I_n$ ideali di A. Allora valgono le seguenti:*

- $P \supseteq \bigcap_{j=1}^{n} I_j \Rightarrow \exists \underline{j} \mid P \supseteq I_{\underline{j}}$;
- $P = \bigcap_{j=1}^{n} I_j \Rightarrow \exists \underline{j} \mid P = I_{\underline{j}}$.

Dimostrazione. Supponiamo che $\forall i \ P \not\supseteq I_i$; mostriamo che $P \not\supseteq \bigcap_{i=1}^{n} I_i$. Poichè $\forall i = 1, ..., n \ \ \exists x_i \in I_i \mid x_i \notin P$, abbiamo

$$x_1 \cdots x_n \in \prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i,$$

ma

$$P \not\supseteq x_1 \cdots x_n \Rightarrow P \not\supseteq \bigcap_{i=1}^{n} I_i.$$

Infine: $P = \bigcap_{i=1}^{n} I_i \ \Rightarrow \ I_{\underline{i}} \subseteq P = \bigcap_{i=1}^{n} I_i \subseteq I_{\underline{i}}$. □

Lemma 1.0.2 (Lemma di Scansamento)**.** *Siano $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ ideali primi, e $I \subseteq A$ ideale. $I \subseteq \bigcup_{j=1}^{n} \mathfrak{p}_j \Rightarrow I \subseteq \mathfrak{p}_j$ per qualche j.*

Dimostrazione. Dimostriamo per induzione su n la contronominale.

P.B. Se $n = 1$, non c'è nulla da dimostrare.

P.I. Assumiamolo vero per $n-1$, e supponiamo che $I \not\subseteq \mathfrak{p}_i \ \forall i = 1, ..., n$. Per ipotesi induttiva, per ogni unione di $n-1$ ideali primi scelti tra i $\mathfrak{p}_j$, I non è contenuto in essa; quindi, in particolare

$$I \not\subseteq \bigcup_{i \neq j} \mathfrak{p}_i \Leftrightarrow \exists x_j \in I - \bigcup_{i \neq j} \mathfrak{p}_i$$

Se $\exists j \in \{1, ...n\}$ tale che $x_j \notin \mathfrak{p}_j$, allora $x_j \in I$ ma non nell'unione di $\mathfrak{p}_i$, quindi abbiamo concluso. Altrimenti, $\forall j = 1, ..., n \ x_j \in \mathfrak{p}_j$. Costruiamo adesso dei particolari elementi:

$$\alpha_j = x_1 \cdots x_{j-1} x_{j+1} \cdots x_n, \quad \beta = \sum_{j=1}^{n} \alpha_j, \quad \beta_j = \beta - \alpha_j = \sum_{i \neq j} \alpha_i$$

Osserviamo che $\forall j = 1, ..., n \ \alpha_j \in \bigcup_{i \neq j} \mathfrak{p}_i - \mathfrak{p}_j$ e $\beta_j \in \mathfrak{p}_j$; ma allora $\beta - \beta_j = \alpha_j \notin \mathfrak{p}_j \Leftrightarrow \beta \notin \mathfrak{p}_j$. Poichè questo deve essere vero per ogni j, β non può stare in nessuno $\mathfrak{p}_j$, quindi nemmeno nell'unione.

□

Diamo ora dei risultati sotto forma di esercizi.

Esercizio. Se A è finito, allora $A = A^* \cup D(A)$.

Esercizio. Sia A anello e $\mathfrak{m}$ un suo ideale massimale. Allora A è *locale*, ovvero ha un solo ideale massimale, se ogni elemento dell'insieme $1 + \mathfrak{m}$ è invertibile.

Supponiamo che $\mathfrak{m}'$ sia un altro ideale massimale in A. Allora $\mathfrak{m} + \mathfrak{m}' = A \Leftrightarrow \exists m \in \mathfrak{m}\ \exists m' \in \mathfrak{m}' \mid 1 = m + m'$. Ma per ipotesi $1 - m = m'$ deve essere invertibile, che è assurdo.

Esercizio. Sia A anello e I ideale. $A[x] \,/\, I[x] \cong (A \,/\, I)[x]$.

Daremo per buone le definizioni di *ideale esteso* e di *ideale contratto*, e preseguiremo enunciando alcune loro proprietà.

Esercizio. *J primo $\Rightarrow$ J^c primo*
J primario $\Rightarrow$ J^c primario
J radicale $\Rightarrow$ J^c radicale
J massimale $\not\Rightarrow$ J^c massimale

Non è in generale vero che l'estensione di un ideale primo è ancora un ideale primo. Un controesempio ci è dato dall'omomorfismo di inclusione $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$.

Ricordiamo il seguente risultato, particolarmente utile quando si affrontano quozienti di anelli per ideali estesi.

Proposizione 1.0.3. *Sia $f : A \to B$ omomorfismo di anelli, $I, J \subseteq A$ ideali. Allora vale sempre che $I^e J^e = (IJ)^e$.*

Dimostrazione. $b \in I^e J^e \Leftrightarrow b = (f(i)b_1)(f(j)b_2), i \in I, j \in J, b_1, b_2 \in B \Leftrightarrow b = f(ij)(b_1 b_2) \Leftrightarrow b \in (IJ)^e$ □

Esercizio. $\sqrt{I}$ massimale $\Rightarrow$ I è primario.

Sia $ab \in I$, con $b \notin \sqrt{I}$; vorremmo mostrare che $a \in I$. $\sqrt{I}$ è massimale $\Rightarrow (\sqrt{I}, b) = (1) \Leftrightarrow 1 = \alpha b + m, m \in \sqrt{I}, \alpha \in A$. Sia n tale che $m^n \in I$; osserivamo che $1 = 1^n = (\alpha b + m)^n \Rightarrow a = a \cdot 1 = a(\alpha b + m)^n \in I + (ab) \subseteq I \Rightarrow a \in I$.

Osservazione. Non è vero, però, che $\sqrt{I}$ primo $\Rightarrow$ I primario.

Esercizio (Esercizio 2.ii, Giugno 2015)**.** Sia $p(x)$ irriducibile in $\mathbb{K}[x]$. É vero che $(p(x), p(y))$ è primo in $\mathbb{K}[x, y]$?

É falso. Il controesempio è x^2+1, irriducibile in $\mathbb{Q}[x]$, ma tale per cui (x^2+1, y^2+1) non è primo in $\mathbb{Q}[x,y]$ in quanto $(x+y)(x-y) \equiv 0\ mod(I)$ ma nessuno dei due sta in I.

Esercizio. Sia A un anello in cui ogni ideale primo è principale. Allora tutti gli ideali sono principali, ovvero A è PIR.

Consideriamo $\Sigma = \{controesempi\} = \{J \subseteq A \text{ ideale} | J \text{ non è principale}\}$. Dimostriamolo per assurdo: supponiamo $\Sigma \neq \emptyset$. Vorremmo applicare il Lemma di Zorn, quindi ordiniamo Σ per inclusione. Ora, se $\{J_i\}_{i\in\mathbb{N}} \subseteq \Sigma$ è una catena, l'ideale J dato dall'unione infinita dei J_i la limita superiormente e deve necessariamente stare in Σ, altrimenti si giunge ad un assurdo. Abbiamo dunque, per Zorn, almeno un elemento massimale; sia esso I. Poichè $I \in \Sigma \Leftrightarrow$ I non è principale $\Rightarrow$ non è primo $\Leftrightarrow \exists\ a, b \notin I \mid ab \in I$. Per massimalità $(I, a) \notin \Sigma \Rightarrow (I, a) = (c), c \in A$; in particolare: $c = i + ah$. Osserviamo però che c'è un altro interessante ideale che contiene strettamente I sul quale possiamo sfruttare l'ipotesi di massimalità di I: $bc = bi + abh \in I \Rightarrow I \subsetneq (I : (c)) \Rightarrow (I : (c)) = (d)$. Perchè ci interessa? Perchè ora dimostreremo che $I = (cd)$, che è chiaramente assurdo.
Sicuramente $(cd) \subseteq I$; ma se $i \in I$, poichè $(I, a) = (c)$, si ha $i = ch \Leftrightarrow h \in (I : (c)) \Leftrightarrow h \in (d) \Rightarrow i = cdhk \Rightarrow I \subseteq (cd)$. Concludiamo dunque che la famiglia di controesempi Σ deve essere vuota.

Vediamo ora due proposizioni sui divisori di zero che ci faranno riflettere in futuro.

Proposizione 1.0.4. *$D(A)$ è unione di ideali primi.*

Dimostrazione. Sia $\Sigma = \{I \subseteq A \mid \forall i \in I, i \in D(A)\}$. Consideriamo l'ordinamento dato dall'inclusione e verifichiamo di poter applicare Zorn. Al solito, se $\{J_i\}_{i\in\mathbb{N}}$ è una catena in Σ, l'ideale J dato dall'unione dei J_i è un ideale $\subseteq \Sigma$ che la maggiora $\Rightarrow$ possiamo scegliere $I \in \Sigma$ massimale. Mostriamo che I è primo. Siano $a, b \notin I \Rightarrow (I, a), (I, b) \notin \Sigma \Rightarrow \exists i + ah \in (I, a), j + bk \in (I, b)$ che non sono divisori di zero. Se, per assurdo, il loro prodotto fosse un divisore di zero $\Rightarrow \exists c \neq 0 \mid (i + ah)(j + bk)c = 0 \Rightarrow i + ah, j + bk$ sarebbero divisori di zero, che è una contraddizione.
In questo modo abbiamo dimostrato che gli elementi massimali della famiglia Σ sono massimali $\Rightarrow D(A)$ è unione di primi, in quanto può essere ottenuto come unione di tali massimali: se $x \in D(A), (x) \in \Sigma \Rightarrow (x) \subseteq I$ per qualcuno degli I massimali in Σ. L'altra inclusione è ovvia, quindi abbiamo l'uguaglianza. □

Proposizione 1.0.5. $D(A) = \bigcup_{a\in A-\{0\}} \sqrt{Ann(a)}$.

Dimostrazione. Osserviamo che

$$\sqrt{D(A)} = D(A) \ \wedge \ \bigcup_{\alpha} \sqrt{E_\alpha} = \sqrt{\bigcup_{\alpha} E_\alpha} \Rightarrow D(A) = \bigcup_{a \in A - \{0\}} \sqrt{Ann(a)},$$

quindi possiamo dimostrare separatamente queste due proprietà.
$D(A) \subseteq \sqrt{D(A)}$. Sia ora $x \in \sqrt{D(A)}$ e sia k il più piccolo naturale tale che $x^k \in D(A)$; allora è evidente che $x \in D(A)$ poichè $x^s \neq 0 \ \forall s < k$.
Veniamo adesso all'altra proprietà:

$$x \in \bigcup_{\alpha} \sqrt{E_\alpha} \Rightarrow \exists k \in \mathbb{N} \wedge \exists \alpha_0 \mid x^k \in E_{\alpha_0} \subseteq \bigcup_{\alpha} E_\alpha \Rightarrow x \in \sqrt{\bigcup_{\alpha} E_\alpha}.$$

E, d'altra parte,

$$x \in \sqrt{\bigcup_{\alpha} E_\alpha} \Rightarrow \exists h : x^h \in \bigcup_{\alpha} E_\alpha \Rightarrow \exists \alpha_0 \mid x^h \in E_{\alpha_0} \Rightarrow x \in \sqrt{E_{\alpha_0}} \subseteq \bigcup_{\alpha} \sqrt{E_\alpha}.$$

□

Teorema 1.1 (Teorema Cinese del Resto)**.** *Sia A anello, $I_1, \cdots, I_n$ ideali a due a due comassimali. Consideriamo la mappa $\phi : A \to A/I_1 \times \cdots \times A/I_n$ tale che $a \longmapsto (a_1, \cdots, a_n)$, dove $a \equiv a_j (I_j) \ \ \forall j = 1, ..., n$. Allora:*

1. $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$
2. *ϕ è surgettiva*
3. *ϕ è iniettiva* $\Leftrightarrow \bigcap_{i=1}^{n} I_i = (0)$

Dimostrazione. Affrontiamo i tre punti separatamente.

1. Proviamo a dimostrarlo per induzione sapendo che $I_i + I_j = 1 \ \forall i \neq j$.

   P.B.: n=2, già visto.

   P.I.: Facciamo vedere che $(\prod_{i=1}^{n-1} I_i, I_n) = (1)$. Gli I_j sono a due a due comassimali, quindi

   $$\forall j \neq n \ \exists \alpha_i \in I_i, \beta_i \in I_n : \alpha_i + \beta_i = 1 \ \forall i = 1, ..., n-1.$$

   Sia $\alpha = \prod_{I=1}^{n-1} \alpha_j \in \prod_{i=1}^{n-1} I_i \Rightarrow \alpha = \prod_{i=1}^{n-1} (1 - \beta_i) \equiv 1 \ (I_n)$, ovvero

   $$\alpha = 1 + \beta, \ \beta \in I_n \ \Rightarrow \ (\prod_{i=1}^{n-1}, I_n) = (1).$$

   Per il passo base: $\left(\prod_{i=1}^{n-1} I_i\right) \cap I_n = \bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_1$.

2. ϕ è surgettiva $\Leftrightarrow \forall (a_1, ..a_n) \in A/I_1 \times \cdots \times A/I_n \ \exists a \in A \mid a \equiv a_j \mod (I_j)$. Per soddisfare questa richiesta costruiremo, per ogni ideale I_j, un elemento $y_j \in A$ tale che $y_j \equiv 1 \mod (I_j)$ e $y_j \equiv 0 \mod (I_i)\ \forall i \neq j$. Facciamo vedere come si costruisce per I_1; per tutti gli altri ideali si fa allo stesso modo. $\forall j \neq 1\ (I_1, I_j) = (1) \Leftrightarrow \exists a_j \in I_1,\ \exists b_j \in I_j$ tale che $1 = a_j + b_j$. Allora
$$\prod_{j=2}^{n}(1 - a_j) = y_1$$
è tale che $y_1 \equiv 1 \mod (I_1)$ e $y_1 \equiv 0 \mod (I_j)\ \forall j \neq 1$.
Se, dunque, disponiamo di $y_1, ..., y_n$ con questa proprietà, scegliamo $a = a_1y_1 + ... + a_ny_n$ e abbiamo l'elemento che cercavamo.

3. Se verifica facilmente che $\prod_{j=1}^{n} I_j$ sia il nucelo di ϕ, e applicando il punto 1 abbiamo la tesi.

□

Corollario 1.1.1. *Abbiamo dunque che* $A/\prod_{i=1}^{n} I_i \cong \prod_{i=1}^{n} A/I_i$

1.1 L'anello $A[x]$

Diamo ora alcuni risultati specifici per l'anello $A[x]$ dei polinomi a coefficenti nell'anello A, e per l'anello delle serie formali $A[|x|]$ a coefficenti nell'anello A. Alcuni verranno presentati come esercizi.

Esercizio. $I \subseteq A$ ideale primo $\Rightarrow I[x] \subseteq A[x]$ è primo.

Proposizione 1.1.1. *Sia* $f(x) = \sum_{j=0}^{n} a_j x^j \in A[x]$.

1. $f(x)$ è invertibile $\Leftrightarrow a_0 \in A^* \wedge a_j \in N(A)\ \forall j \in \{1, \cdots, n\}$
2. $f \in N(A[x]) \Leftrightarrow a_j \in N(A)\ \forall j$
3. $f \in D(A[x]) \Leftrightarrow \exists a \in A - \{0\} \mid af = 0$

Dimostrazione. Dimostriamo una alla volta i tre punti.

1. ($\Leftarrow$) Sia $a_0 \in A^*$ e $a_1, \cdots, a_n \in N(A) \Rightarrow f = a_0 + a_1x + \cdots + a_nx^n =$ invertibile + nilpotente $\Rightarrow f \in A[x]^*$.
($\Rightarrow$) Sia f invertibile, allora:
$$\exists g(x) = \sum_{j=0}^{m} b_j x^j \in A \mid 1 = g(x)f(x) = \sum_{j=0}^{n+m} c_j x^j$$

$$\Rightarrow c_0 = a_0 b_0 = 1 \Rightarrow a_0 \in A^*.$$

Per quel che riguarda gli altri coefficenti osserviamo che: $0 = c_{n+m} = a_n b_m$ e $0 = c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m = a_n(a_n b_{m-1} + a_{n-1} b_m) \Rightarrow a_n^2 b_{m-1} = 0$. Iterando il ragionamento, ovvero moltiplicando c_{n+m-j} per a_n^j, otteniamo che $\forall r \leq n+m-1$ vale che $0 = a_n^{r+1} b_{n-r}$; se dunque $r = m$ allora $a_n^{m+1} b_0 = 0 \Rightarrow a_n \in N(A)$. Per dedurre che anche gli altri coefficenti sono nilpotenti applichiamo questo medesimo ragionamento al polinomio $g(x)(f(x) - a_n x^n) = 1 - g(x) a_n x^n$, che è invertibile in quanto somma di 1 e di un nilpotente.

2. ($\Leftarrow$) Se tutti i coefficenti sono nilpotenti allora esiste un k naturale abbastanza grande tale che f^k si annulli - dipenderà dai vari indici di nilpotenza. ($\Rightarrow$) Sia ora f nilpotente $\Rightarrow xf(x) \in N(A[x]) \Rightarrow 1 + xf \in A[x]^* \Rightarrow a_j \in N(A)\ \forall j \in \{0, \cdots, n\}$ per il punto precedente.

3. Una implicazione è ovvia. Per l'altra consideriamo g polinomio di grado minimo che annulla f. Allora...

□

Ribadiamo il risultato utilizzato e dimostrato in quest'ultimo punto della proposizione:

Esercizio. Per ogni anello A vale che $N(A[x]) = \mathfrak{J}(A[x])$.

Arrivati a questo punto, ci piacerebbe formalizzare un algoritmo per decidere l'appartenenza di un polinomio in $\mathbb{K}[x_1, \ldots, x_n]$ ad un certo ideale; come vedremo, il problema richiede l'introduzione di basi particolari per gli ideali. Ad ogni modo, possiamo già risolvere il problema di appartenenenza al radicale.

Proposizione 1.1.2 (Test di appartenenza al Radicale)**.** *Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ e $I = (f_1, \cdots, f_k)$ ideale. Allora*

$$f(\underline{x}) \in \sqrt{I} \Leftrightarrow (1) = (I, 1 - tf(\underline{x})) \subseteq \mathbb{K}[x_1, \ldots, x_n][t].$$

Dimostrazione. Dimostriamo le due inclusioni.

($\subseteq$) $f \in \sqrt{I}$. $1 = f^m t^m + (1 - t^m f^m) = t^m f^m + (1 - tf) \sum_{i=0}^{m-1} t^i f^i \Rightarrow (I, 1 - tf) = (1)$;

($\supseteq$) $(1) = (I, 1 - tf(\underline{x})) \Rightarrow 1 = \sum_{i=1}^{k} h_i(\underline{x}, t) f_i(\underline{x}) + (1 - tf) h(\underline{x}, t)$. Poichè questa espressione è indipendente dal valore delle indeterminate, è lecito

sostituire $\frac{1}{f}(\underline{x})$ a t e ottenere

$$1 = \sum_{i=1}^{k} h_i(\underline{x}, \frac{1}{f(\underline{x})}) f_i(\underline{x}).$$

Sfruttando il minimo comune multiplo possiamo scrivere

$$1 = \sum_{i=1}^{k} \frac{\overline{h_i}(\underline{x}) f_i(\underline{x})}{f(\underline{x})^r} \Leftrightarrow f(\underline{x})^r = \sum_{i=1}^{k} \overline{h_i}(\underline{x}) f_i(\underline{x}) \Rightarrow f(\underline{x}) \in \sqrt{I}.$$

□

Proposizione 1.1.3 (Facoltativo)**.** *Sia $I = (f)$, con $f \in \mathbb{K}[x_1, \ldots, x_n]$. Se $f = c f_1^{a_1} \cdots f_k^{a_k}$ è la fattorizzazione in irriducibili di f, allora: $\sqrt{I} = \sqrt{(f)} = (f_1 \cdots f_k)$*

Dimostrazione. ($\supseteq$) Mostriamo che $f_1 \cdots f_k \in \sqrt{I}$. Scegliamo N più grande del massimo degli $a_j \Rightarrow f^N = f_1^{N-a_1} \cdots f_k^{N-a_k} f$. ($\subseteq$). Sia ora $g \in \sqrt{I} \Leftrightarrow \exists n \in \mathbb{N} \mid g^n \in I = (f) \Leftrightarrow g^n = f \Rightarrow \forall i \ f_i \mid g^m \Rightarrow f_i \mid g \Rightarrow g \in (f_1 \cdots f_k)$. □

1.1.1 Gli ideali primi di $\mathbb{Z}[x]$

Sia ora $A = \mathbb{Z}$. Sfruttiamo i risultati precedenti per caratterizzare gli ideali primi dell'anello dei polinomi a coefficenti interi. Per ora ne conosciamo già alcuni:

- $\mathbb{Z}$ $UFD \Rightarrow \mathbb{Z}[x]$ UFD, dunque irriducibile $\Leftrightarrow$ primo;
- $\forall (p)$ ideale primo in $\mathbb{Z}$, la sua estensione $(p)[x]$ è un ideale primo di $\mathbb{Z}[x]$ perchè $\mathbb{Z}[x] \,/\, (p)[x] \cong \mathbb{Z} \,/\, (p)[x]$ è integro;
- $(p, g(x))$ con p primo in $\mathbb{Z}$ e $g(x)$ irriducibile modulo p è primo poichè $\mathbb{Z}[x] \,/\, (p, g(x)) \cong ((\mathbb{Z} \,/\, (p))[x]) \,/\, (\overline{g}(x))$ è integro in quanto $\overline{g}(x)$ è irriducible $\Leftrightarrow$ primo in $\mathbb{Z} \,/\, (p)$.

Ora vorremmo dimostrare che gli ideali primi sono tutti e soli quelli appena elencati. Per farlo sfrutteremo le proprietà della contrazione rispetto alla mappa di inclusione $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ e quello che già sappiamo su $\mathbb{Z}$.
Iniziamo osservando che $\forall I \subseteq \mathbb{Z}[x]$ ideale primo vale che $I^c = I \cap \mathbb{Z} =$ ideale primo di $\mathbb{Z}$, dunque I^c può essere della forma (0) o (p) con p primo.

- $I \cap \mathbb{Z} = (p) \Rightarrow I^{ce} = (p)[x] \subseteq I$ perchè in generale $I^{ce} \subseteq I$. Ma allora $\mathbb{Z}[x] \,/\, I \cong (\mathbb{Z}[x] \,/\, (p)[x]) \,/\, (I \,/\, (p)[x])$. I è primo $\Rightarrow$ entrambi i quozienti sono integri; ma allora, poichè il quoziente $(\mathbb{Z} \,/\, (p))[x] \,/\, (I \,/\, (p)[x])$ deve essere integro, I non può che essere della forma $I = (p)[x]$ o $I = (\overline{g}(x))$ con $\overline{g}(x)$ irriducibile modulo p.

- Supponiamo ora $I^c = I \cap \mathbb{Z} = (0)$. Scegliamo $f \in I$ irriducibile e dimostriamo che $\forall g \in I \ f|g$. Se per assurdo $\exists g \in I \mid f \not| g \Rightarrow$ in $\mathbb{Q}[x]$ vale $gcd(f,g) = 1 \wedge \exists A(x), B(x) \in \mathbb{Q}[x] \mid A(x)f(x) + B(x)g(x) = 1$; moltiplicando per il minimo comune multiplo otteniamo $\overline{A(x)}f(x) + \overline{B(x)}g(x) = k, k \in \mathbb{Z}$, che è assurdo perchè $I^c = (0)$.

1.2 L'anello $A[|x|]$

Passiamo ora all'anello delle serie formali a coefficenti nel generico anello A. Anche in questo caso caratterizzeremo invertibili e nilpotenti.Tratteremo inoltre il radicale di jacobson e daremo delle informazioni sulla contrazione degli ideali massimali.

Proposizione 1.2.1. *Sia* $p(x) = \sum_{j=0}^{\infty} a_j x^j \in A[|x|]$. *Allora valgono i seguenti fatti.*

1. $p(x) \in A[|x|]^* \Leftrightarrow a_0 \in A^*$;
2. $p(x) \in N(A[|x|]) \Rightarrow a_j \in N(A) \ \forall j \in \mathbb{N}$;
3. $p(x) \in \mathfrak{J}A([x]) \Leftrightarrow a_0 \in \mathfrak{J}(A)$;
4. *la contrazione di un ideale massimale* $\mathfrak{m}$ *è ancora un ideale massimale, e inoltre vale che* $\mathfrak{m} = (\mathfrak{m}^c, x)$.

Dimostrazione.

1. ($\Rightarrow$) Se $\exists \ g(x) = \sum_{j=0}^{\infty} b_j x^j \in A[|x|] \mid p(x)g(x) = 1 \Rightarrow a_0 b_0 = 1 \Rightarrow a_0 \in A^*$. ($\Leftarrow$) Supponiamo di voler determinare i coefficenti b_j di una serie formale $g(x)$ tale che $p(x)g(x) = 1$. In primo luogo serve $a_0 \in A^*$, cosicchè $a_0 b_0 = 1$; ora dimostriamo che è sufficiente poter scegliere $b_0 = a_0^{-1}$ per determinare gli altri coefficenti. Ecco, facciamo finta che l'ho dimostrato perchè dovrei farvi vedere che un sistema infinito ha soluzione e servono veramente tanti tanti tanti indici, e non ho voglia. Fidatevi.

2. $p(x) \in N(A[|x|]) \Leftrightarrow \exists k \in \mathbb{N} \mid p^k = 0 \Rightarrow a_0 \in N(A)$. Ma allora $p(x) - a_0 \in N(A[|x|]) \Rightarrow a_1 \in N(A)$. Iterando il ragionamento si ha che tutti i coefficenti sono nilpotenti. Non è tuttavia vero il viceversa - a breve vederemo un controesempio.

3. $p \in \mathfrak{J}(A[|x|]) \Leftrightarrow \forall g \in A[|x|] \ 1 - pg \in A[|x|]^* \Leftrightarrow 1 - a_0 b \in A^* \ \forall b \in A \Leftrightarrow a_0 \in \mathfrak{J}(A)$.

4. Sia $\mathfrak{m} \subseteq A[|x|]$. Osserviamo innanzitutto che $x \in \mathfrak{m}$, altrimenti $(\mathfrak{m}, x) = (1) \Rightarrow \exists f \in \mathfrak{m}, g, h \in A[|x|]$ tali che $1 = fg + hx = f_0 g_0 + x\overline{h}$, dove f_0, g_0 indicano i termini noti di f e g. A questo punto avremmo che

f è invertibile perchè f_0 lo è, che è assurdo in quanto $f \in \mathfrak{m} \subsetneq A[|x|]$. Consideriamo ora $\mathfrak{n} = \{a \in A \mid a + \sum_{i=0}^{k} a_i x^i \in A[|x|]\}$. É immediato dimostrare che $\mathfrak{n}$ è un ideale, e per massimalità segue che $(\mathfrak{n}, x) = \mathfrak{m} \Rightarrow \mathfrak{n} = \mathfrak{m}^c$. Infine abbiamo che $\mathfrak{n}$ è massimale perchè $A[|x|] \,/\, \mathfrak{m} \;\cong\; A \,/\, \mathfrak{n}$.

□

Capitolo 2

Le Basi di Gröbner

Le basi di Gröbner sono di nostro interesse poichè ci aiutano a risolvere due problemi fondamentali nell'anello $\mathbb{K}[x_1, \ldots, x_n]$. In particolare, ci aiutano a dare risposta alle seguenti domande:

- scelti il polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ e l'ideale $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, quando è vero che $f \in I$?
- dati $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideali, quando è vero che $I = J$?

L'esistenza di basi si Gröbner ci permetterà inoltre di dire che ogni ideale di $\mathbb{K}[x_1, \ldots, x_n]$ è finitamente generato. In previsione di ciò, è bene soffermarsi sulle seguenti nozioni.

Definizione 2.0.1. *$I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ si dice **ideale monomiale** se $\exists E \subseteq \mathbb{N}^n$ tale che $I = \{X^\alpha \mid \alpha \in E\}$, dove con X^α si intende $x_1^{a_1} \cdots x_n^{a_n}$, con $X = x_1 \cdots x_n$ e $\alpha = (a_1, ..., a_n)$.*

Osserviamo dunque che un monomio $m = X^\beta$ sta in I se $\exists \alpha \in \mathbb{N}^n$ tale che $X^\alpha | X^\beta$, ovvero $\beta - \alpha \in \mathbb{N}$.

Proposizione 2.0.1. *Sia $f = \sum c_\beta X^\beta \in \mathbb{K}[x_1, \ldots, x_n]$ e I ideale monomiale. Allora*

$$f \in I \Leftrightarrow \forall \beta \; c_\beta X^\beta \in I.$$

Cerchiamo ora di individuare quali sottoinsiemi di $\mathbb{N}^n$ ci sono utili per rappresentare gli ideali monomiali.

Definizione 2.0.2. *$E \subseteq \mathbb{N}^n, E \neq \emptyset$ si dice $\mathfrak{E}$-sottoinsieme se $\forall \alpha \in E, \forall \beta \in \mathbb{N}^n$ si ha che $\alpha + \beta \in E$*[1].

[1] La somma è intesa componente per componente.

Sappiamo che $\mathbb{N}$ è un insieme che gode della proprietà del minimo. Per capire che forma assuma questa proprietà nel caso degli $\mathfrak{E}$-sottoinsiemi, introduciamo la seguente definizione.

Definizione 2.0.3. *$F \subseteq E$, $E \subseteq \mathbb{N}^n$ E-sottoinsieme, è detta **frontiera** se $\forall \alpha \in E \ \exists \gamma \in F \wedge \exists \beta \in \mathbb{N}^n$ tali che $\alpha = \beta + \gamma$.*

Teorema 2.1 (Lemma di Dickson)**.** *$\forall E \subseteq \mathbb{N}^n$ $\mathfrak{E}$-sottoinsieme, E ha una frontiera finita. Equivalentemente, ogni ideale monomiale è finitamente generato.*

Dimostrazione. Dimostriamolo per induzione su n.

P.B. Sia $n = 1$. La frontiera minimale esiste per il principio del buon ordinamento.

P.I. Supponiamo che sia vero per n e scegliamo $E \subseteq \mathbb{N}^{n+1}$. Sia $\pi : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}^n$ la mappa che dimentica l'ultima coordinata. Mostriamo che $\pi(E)$ è un $\mathfrak{E}$-sottoinsieme di $\mathbb{N}^n$: sia $\pi(\alpha) \in \pi(E)$ e $\gamma \in \mathbb{N}^n$; allora $\pi(E) + \gamma = \pi(\alpha + (\gamma, 0))$. Sia dunque F frontiera finita di $\pi(E)$. Scegliamo delle controimmagini per gli elementi di F e chiamiamo $F_0 = \{\gamma_1, ..., \gamma_k\}$ l'insieme di tali controimmagini. Denotiamo con $\overline{a}$ il massimo tra le ultime componenti dei γ_i al variare di i. Consideriamo ora

$$E_a = E \cap (\mathbb{N}^n \times \{a\}) = \{x \in E \mid x = (x_1, ..., x_n, a)\} \ \forall a < \overline{a}.$$

In modo analogo a prima si dimostra che $\pi(E_a)$ è un $\mathfrak{E}$-sottoinsieme di $\mathbb{N}^n$ per ogni $a < \overline{a}$, dunque ne possiamo scegliere una frontiera finita e una sua controimmagine, che chiameremo F_a. Dimostriamo ora che l'insieme finito

$$F_0 \cup \left(\bigcup_{a<\overline{a}} F_a \right)$$

è una frontiera di E. Sia $\beta \in \mathbb{N}^{n+1}$. Se $\beta_{n+1} > \overline{a}$, allora $\exists \alpha \in F_0$ tale che $\beta - \alpha \in \mathbb{N}^n$; se invece $\beta_{n+1} = a < \overline{a}$, allora esiste $\alpha \in F_a$ tale che $\beta - \alpha \in \mathbb{N}^n$.

□

Si può inoltre dimostrare che esiste una frontiera minimale e che la cardinalità di tale frontiera è unica.

Prima di passare alle basi di Gröbner sarebbe opportuno parlare di ordinamenti monomiali e divisione tra polinomi. Per il momento questi argomenti verrranno messi da parte, con la speranza di riuscire ad integrarli.

Se $F = \{f_1, \dots, f_s\} \subseteq \mathbb{K}[x_1, \dots, x_n]$, e scegliamo $f \in \mathbb{K}[x_1, \dots, x_n]$, ridurre f modulo F produce una scrittura del tipo

$$f \xrightarrow{F} r \Leftrightarrow f = \sum_{j=1}^{s} u_j f_j + r$$

con r ridotto, ovvero che verifica una delle seguenti condizioni:

- $r = 0$;
- $r = \sum_{\alpha} r_\alpha X^\alpha$, $\forall \alpha$ tale che $r_\alpha \neq 0 \Rightarrow r_\alpha X^\alpha \notin (lt(f_1), \dots, lt(f_s))$.

Detto ciò, iniziamo a parlare nello specifico di cosa sia una base di Gröbner.

2.1 Caratterizzazione delle Basi di Gröbner

Supponiamo di avere $I \subseteq \mathbb{K}[x_1, \dots, x_n]$. Vorremmo individuare un insieme di polinomi $G \subseteq I$ tale che $\forall f \in \mathbb{K}[x_1, \dots, x_n]$ valga $f \in I \Leftrightarrow f \xrightarrow{G} 0$.
Iniziamo con l'osservare che ad ogni ideale I possiamo associare l'ideale monomiale $LT(I) = (lt(f) | f \in I)$. Trattandosi, appunto, di un ideale monomiale, sappiamo che $\exists m_1, \dots, m_s$ tali che $LT(I) = (m_1, \dots, m_s)$, ovvero sappiamo che possiede una frontiera finita; e se la scegliamo minimale, sappiamo anche che gli m_j sono anche univocamente determinati. Possiamo inoltre scegliere $\{g_1, \dots, g_s\} \in I$ tali che $\forall j \in \{1, \dots, s\}$ $m_j = lt(g_j)$.
Osserviamo subito che i polinomi g_j **non** sono univocamente determinati.

Definizione 2.1.1. *Diciamo che $G = \{g_1, \dots, g_s\} \subseteq I$ ideale di $\mathbb{K}[x_1, \dots, x_n]$ è una Base di Gröbner di I se vale $LT(I) = LT(G)$.*

Proposizione 2.1.1. *Le seguenti condizioni sono equivalenti e forniscono una prima caratterizzazione per le Basi di Gröbner.*

1. *$LT(G) = LT(I)$;*
2. *$f \in I \Leftrightarrow f \xrightarrow{G} 0$;*
3. *$f \in I \Leftrightarrow f = \sum_{j=1}^{s} u_j g_j$ con i g_i in G e $Deg f \geq Deg(u_j g_j)$ se $u_j g_j \neq 0$.*

Dimostrazione. Il punto 3) è essenzialmente un'osservazione, quindi ci dedicheremo a mostrare l'equivalenza tra il primo e il secondo punto.

1) $\Rightarrow$ 2) Se $f \xrightarrow{G} 0 \Leftrightarrow f = \sum_{j=1}^{s} u_j g_j \Rightarrow f \in I$. Supponiamo ora $f \in I$ e $f \xrightarrow{G} r$, $r \neq 0$. Allora $r = f - \sum_{j=1}^{s} u_j g_j \in I \Rightarrow \exists i : lt(g_i) | lt(r)$, che è assurdo a meno che $r = 0$.

2) $\Rightarrow$ 1) $\forall f \in I$ vale che $f \xrightarrow{G} 0 \Leftrightarrow f = \sum_{j=1}^{s} u_j g_j$. Possiamo supporre di aver ridotto f sfruttando l'algoritmo di divisione, quindi possiamo affermare che $Deg(f) \geq Deg(u_i g_i)\ \forall i$ tale che $u_i g_i \neq 0$. Inoltre, $Deg(h_1 + h_2) \leq Deg(h_1) + Deg(h_2)$, da cui

$$Deg(u_i g_i) \leq Deg(f) = Deg \sum_i u_i g_i \leq \max_i Deg(u_i g_i).$$

Ma allora esiste un addendo g_i con medesimo multigrado di f che verifica $lt(g_i)|lt(f)$.

□

Seguono degli importanti Corollari:

Corollario 2.1.1. *Sia $G \subseteq I$ base di Gröbner, $G = \{g_1, \ldots, g_n\} \Rightarrow I = (g_1, \ldots, g_n)$.*

Corollario 2.1.2 (Teorema della Base di Hilbert)**.** *$\forall I \in \mathbb{K}[x_1, \ldots, x_n], I$ è finitamente generato.*

Corollario 2.1.3. *G base di Gröbner per I, allora $\forall f \in \mathbb{K}[x_1, \ldots, x_n]$, se $f \xrightarrow{G} r$, r è unico.*

Dimostrazione. Se ci fossero due resti, r_1 e r_2, basta ridurre la loro differenza con G e si conclude facilmente che deve essere 0. □

Sorge ora spontanea una domanda sull'unicità della base di Gröbner. Sfortunatamente, tale proprietà non è soddisfatta. Se però per ogni elemento della frontiera minimale scegliamo un solo elemento della base di Gröbner con tale leading term, riusciamo a dare la definizione di base **minimale**. Per guadagnare l'unicità, invece, è necessario ridurre anche tutti i vari monomi che compaiono negli elementi della base.

Definizione 2.1.2. *$G = \{g_1, \ldots, b_n\}$ base di Gröbner si dice **ridotta** se $\forall i \neq j$ $lt(g_i)$ non divide $lt(g_j)$ e se $\forall j = 0, \ldots, s$, g_j è ridotto rispetto a $G - \{g_j\}$. Per semplicità richiediamo inoltre che i leading coefficents siano tutti uguali a 1.*

Esercizio. Siano $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideali tali che $I \subseteq J$ e $LT(I) = LT(J)$. É vero che $I = J$?
Siano G_I, G_J basi di Gröbner rispettivamente di I e di J, allora vale $LT(G_I) = LT(I) = LT(J) = LT(G_J)$. Abbiamo già un'inclusione per ipotesi; mostriamo l'altra. Sia $f \in J$; riduciamolo rispetto a G_I e otteniamo $f \xrightarrow{G_I} r$ con r ridotto. Supponiamo, per assurdo, che $r = \sum_\alpha r_\alpha x^\alpha \neq 0$; ma $I \subseteq J \Rightarrow r \in J \Leftrightarrow r \xrightarrow{G_I} 0 \Rightarrow r \in LT(J) = LT(I)$ assurdo poichè avevamo supposto r ridotto rispetto a G_I.

2.2 Teorema di Eliminazione

In questa sezione illustreremo alcune proprietà dell'ordinamento lessicografico.

Teorema 2.2 (Teorema di Eliminazione)**.** *Consideriamo $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideale. Fissiamo l'ordinamento lessicografico con $x_1 > \cdots > x_n$ e denotiamo con G una base di Gröbner di I. $\forall l = 1, \cdots, n$ definiamo $I_l = I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$ e lo chiamiamo l-esimo ideale di eliminazione. Inoltre denotiamo $G_l = G \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$. Allora, sotto queste ipotesi, G_l è base di Gröbner di I_l.*

Dimostrazione. La tesi è che $LT(I_l) = LT(G_l)$. Dimostriamo le due inclusioni.

- ($\supseteq$) Se $g \in G_l = G \cap \mathbb{K}[x_{l+1}, \cdots, x_n] \subseteq I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$, quindi $lt(g) \in LT(I)$.
- ($\subseteq$) Sia $m \in LT(I_l) \Leftrightarrow \exists f \in I_l \mid f = m+$ monomi più piccoli secondo il lex. $f \in I_l \Rightarrow \exists g \in G \mid lt(g) | lt(f)$. Per concludere ci serve che $lt(g) \in \mathbb{K}[x_{l+1}, \cdots, x_n]$, ma questo è vero per le proprietà del lex, giacché se in $lt(g)$ comparisse qualche potenza positiva di qualche variabile con indice minore di $l+1$, allora $lt(g)$ non potrebbe dividere f, in quanto $f \in I_l$. In conclusione $g \in G_l$.

□

Grazie a questa proprietà dell'ordinamento lessicografico, e più nello specifico al teorema appena dimostrato, potremo dare degli algoritmi per il calcolo di alcuni tipi di ideali.

Proposizione 2.2.1 (Intersezione di Ideali)**.** *Siano $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Sia $i : \mathbb{K}[x_1, \ldots, x_n] \hookrightarrow \mathbb{K}[t, x_1, \cdots, x_n]$. Allora $(tI, (1-t)J) \cap \mathbb{K}[x_1, \ldots, x_n] = I \cap J$.*

Dimostrazione. Dimostriamo le due inclusioni.

- ($\subseteq$) $f \in I \cap J, f = tf + (1-t)f \in (tI, (1-t)J) \Rightarrow f \in (tf, (1-t)J) \cap \mathbb{K}[x_1, \ldots, x_n]$
- ($\supseteq$) $f \in tI + (1-t)J \Leftrightarrow \exists g(\underline{x}, t) \in tI,\ h(\underline{x}, t) \in (1-t)J \mid f = g(\underline{x}, t) + h(\underline{x}, t)$. Osserviamo che $g(\underline{x}, 0), h(\underline{x}, 0) \in J$ e che $f(\underline{x}) = g(\underline{x}, 1) \in I \Rightarrow f \in I \cap J$.

□

Proposizione 2.2.2 (Colon)**.** *Sia $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideale e sia f un qualsiasi polinomio in $\mathbb{K}[x_1, \ldots, x_n]$. Allora $I : (f) = \frac{1}{f}(I \cap (f)) \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Precisamente, se $I = (f_1, \cdots, f_k)$ e $J = (g_1, \cdots, g_h)$, allora:*

$$(tI, (1-t)J) = (tf_1, \cdots, tf_k, (1-t)g_1, \cdots, (1-t)g_h).$$

Dimostrazione. Facciamo vedere le due inclusioni.

($\subseteq$) $g \in (I : (f)) \Leftrightarrow gf \in I \cap (f)$

($\supseteq$) $g \in \frac{1}{f}(I \cap (f)) \Leftrightarrow gf \in (I \cap (f)) \subseteq I \Rightarrow g \in (I : (f))$

□

Capitolo 3

Varietà Affini

Introduciamo ora il concetto di Varietà Affine.

Definizione 3.0.1. *Dato $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, chiamiamo Varietà Affine l'insieme* $\mathbb{V}(I) = \{\alpha \in \mathbb{K}^n | f(\alpha) = 0 \ \forall f \in I\}$

Vogliamo inoltre definire una sorta di operazione inversa, ovvero associare ad una varietà un ideale. A tal proposito definiamo le seguenti mappe:

$$\begin{aligned} \mathbb{V} :&\{\text{ideali di } \mathbb{K}[x_1, \ldots, x_n]\} \longrightarrow P(\mathbb{K}^n) \\ &I \longmapsto \mathbb{V}(I) \end{aligned}$$

$$\begin{aligned} \mathcal{I} :&P(\mathbb{K}^n) \longrightarrow \{\text{ideali di } \mathbb{K}[x_1, \ldots, x_n]\} \\ &V \longmapsto \mathcal{I}(V) \end{aligned}$$

dove $\mathcal{I}(\mathbb{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] | \ \forall \alpha \in \mathbb{V} \ f(\alpha) = 0\}$e con $P(\mathbb{K}^n)$ si intende l'insieme delle parti di $\mathbb{K}^n$.
Illustriamo subito alcune proprietà di queste mappe.

Proposizione 3.0.1. *Siano V, W varietà affini, $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideali. Allora valgono le seguenti proprietà:*

1. $I \subseteq J \Rightarrow \mathbb{V}(I) \supseteq \mathbb{V}(J)$
2. $V \subseteq W \Leftrightarrow \mathcal{I}(V) \supseteq \mathcal{I}(W)$, *e vale l'uguale se e solo se vale da ambo i lati*
3. $I \subseteq \mathcal{I}(\mathbb{V}(I))$
4. $V = \mathbb{V}(\mathcal{I}(V))$
5. $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$
6. $\mathbb{V}(IJ) = \mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J)$

7. $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$
8. $\mathcal{I}(V \cup W) = \mathcal{I}(V) \cap \mathcal{I}(W)$
9. $V = \{\alpha = (a_1, \ldots, a_n)\} \Rightarrow \mathcal{I}(V) = (x_1 - a_1, \ldots, x_n - a_n)$ *ideale massimale*
10. *Ogni catena discendente di varietà si stabilizza.*

Dimostrazione.

1. Sia $\alpha \in \mathbb{V}(J) \Rightarrow \forall f \in J \ f(\alpha) = 0$; $I \subseteq J$, quindi $\forall g \in I \ g(\alpha) = 0$, da cui $\mathbb{V}(J) \subseteq \mathbb{V}(I)$.
2. ($\Rightarrow$) Supponiamo $V \subseteq W$ e scegliamo $f \in \mathcal{I}(W) \Leftrightarrow \forall \alpha \in W \ f(\alpha) = 0$; ma $V \subseteq W$, quindi $\forall \beta \in V$ vale $f(\beta) = 0$, da cui $f \in \mathcal{I}(V)$.
   ($\Leftarrow$) Supponiamo $\mathcal{I}(W) \subseteq \mathcal{I}(V)$ e scegliamo $\alpha \in V$. $\forall f \in \mathcal{I}(V)$ vale $f(\alpha) = 0$, quindi anche $\forall g \in \mathcal{I}(W) \ g(\alpha) = 0$, da cui $\alpha \in W$.
   L'ugualianza vale in entrambi i casi poichè se vale l'uguale da uno dei due lati si possono dedurre le due inclusioni sfruttando quanto appena dimostrato.
3. $\mathcal{I}(\mathbb{V}(I)) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \forall \alpha \in \mathbb{V}(I) \ f(\alpha) = 0\}$, ma $\mathbb{V}(I) = \{\alpha \in \mathbb{K}^n \mid \forall g \in I, g(\alpha) = 0\}$, quindi $I \subseteq \mathcal{I}(\mathbb{V}(I))$.
4. $\alpha \in V \Leftrightarrow \forall g \in \mathcal{I}(V) \ f(\alpha) = 0 \Rightarrow \alpha \in \mathbb{V}(\mathcal{I}(V))$. Viceversa, $\beta \in \mathcal{I}(\mathbb{V}(I)) \Leftrightarrow \forall g \in \mathcal{I}(V) \ g(\beta) = 0 \Rightarrow \beta \in V$.
5. $I \subseteq I + J$, $J \subseteq I + J \Rightarrow \mathbb{V}(I + J) \subseteq \mathbb{V}(I) \cap \mathbb{V}(J)$. D'altra parte, se $\alpha \in \mathbb{V}(I) \cap \mathbb{V}(J) \Rightarrow \forall h = f + j \in I + J$ vale $h(\alpha) = f(\alpha) + g(\alpha) = 0 + 0 = 0$, quindi $\mathbb{V}(I) \cap \mathbb{V}(J) \subseteq \mathbb{V}(I + J)$.
6. Cominciamo osservando che $IJ \subseteq I \cap J \subseteq I, J$, quindi $\mathbb{V}(IJ) \supseteq \mathbb{V}(I \cap J) \supseteq \mathbb{V}(I) \cup \mathbb{V}(J)$. D'altra parte, se $\alpha \in \mathbb{V}(IJ) \Rightarrow \forall i \in I, j \in J$, $ij(\alpha) = i(\alpha)j(\alpha) = 0 \Rightarrow i(\alpha) = 0 \vee j(\alpha) = 0$ per integrità di $\mathbb{K}[x_1, \ldots, x_n]$, quindi $\alpha \in \mathbb{V}(I) \cup \mathbb{V}(J)$.
7. $I \subseteq \sqrt{I} \Rightarrow \mathbb{V}(I) \supseteq \mathbb{V}(\sqrt{I})$. D'altra parte, se $\alpha \in \mathbb{V}(I)$ e $f \in \sqrt{I} \Leftrightarrow \exists n \in \mathbb{N} \mid f^n \in I$, allora $f^n(\alpha) = f(\alpha)^n = 0 \Rightarrow f(\alpha) = 0$, ovvero $\alpha \in \mathbb{V}(\sqrt{I})$.
8. $V, W \subseteq V \cup W \Rightarrow \mathcal{I}(V \cup W) \subseteq \mathcal{I}(V) \cap \mathcal{I}(W)$. Ad ogni modo, se $f \in \mathcal{I}(V) \cap \mathcal{I}(W) \Rightarrow \forall \alpha \in V \cup W \ f(\alpha) = 0 \Rightarrow f \in \mathcal{I}(V \cup W)$.
9. Osserviamo che $(x_1 - a_1, ..., x_n - a_n)$ è contenuto in $\mathcal{I}(V)$, ma che è anche massimale, quindi deve valere l'uguaglianza.
10. Se $V_1 \supseteq V_2 \supseteq ...$ è una catena discendente di varietà, possiamo considerare $\mathcal{I}(V_1) \subseteq \mathcal{I}(V_2) \subseteq ...$ catena ascendente di ideali in $\mathbb{K}[x_1, \ldots, x_n]$. Poichè $\mathbb{K}[x_1, \ldots, x_n]$ è noetheriano, sappiamo che questa catena stabilizza, e per la proprietà 2 possiamo dire che anche la catena di varità stabilizza.

□

Un'altra importante proprietà, sotto certi aspetti analoga al lemma di decomposizione per ideali, è la seguente.

Proposizione 3.0.2. *Siano $I, J, H \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideali. Allora vale $\mathbb{V}(I, JH) = \mathbb{V}(I, J) \cup \mathbb{V}(I, H)$.*

Dimostrazione. Come al solito cominciamo osservando che $(I, JH) \subseteq (I, J) \cap (I, H) \Rightarrow \mathbb{V}(I, JH) \supseteq \mathbb{V}((I, J) \cap (I, H)) = \mathbb{V}(I, JH)$; ma è anche vero che $\mathbb{V}(I + JH) = \mathbb{V}(I) \cap \mathbb{V}(JH) = \mathbb{V}(I) \cap (\mathbb{V}(J) \cup \mathbb{V}(H)) = (\mathbb{V}(I) \cap \mathbb{V}(J)) \cup (\mathbb{V}(I) \cap \mathbb{V}(H)) = \mathbb{V}(I, J) \cup \mathbb{V}(I, H)$. □

Esercizio. Siano $I = (x - y + z^2, y - z - 1, z^3)$, $J = (x^2 - z - 1, y^2 + z - 1, z(z - 1))$. Chi sono $\mathbb{V}(I)$ e $\mathbb{V}(J)$? E cosa possiamo dire su $\sqrt{I}$ e $\sqrt{J}$?
$\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$, dunque $z \in \sqrt{I} \Rightarrow \mathbb{V}(I) = \mathbb{V}(x - y, y - 1, z) = \{(1, 1, 0)\}$. Invece $\mathbb{V}(J) = \mathbb{V}(x^2 - 1, y^2 - 1, z) \cup \mathbb{V}(x^2 - 2, y^2, z - 1) = \mathbb{V}(x - 1, y - 1, z) \cup \mathbb{V}(x - 1y + 1, z) \cup \mathbb{V}(x + 1, y - 1, z) \cup \mathbb{V}(x + 1, y + 1, z) \cup \mathbb{V}(x - \sqrt{2}, y, z - 1) \cup \mathbb{V}(x + \sqrt{2}, y, z - 1)$, dunque $\mathbb{V}(I) \subseteq \mathbb{V}(J) \Rightarrow \sqrt{I} \neq \sqrt{J}$ per le proprietà 2 e 7.

3.1 Hilbert's Nullstellensatz

Dimostreremo ora l'importantissimo teorema della parete.

Lemma 3.1.1. *Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$, con $\mathbb{K} = \overline{\mathbb{K}}$, tale che $deg(f, x_1) > 0$. Allora esiste un cambio di coordinate lineare del tipo*

$$\overline{x_1} = x_1, \quad \overline{x_2} = (x_2 + c_2\overline{x_1}), \quad \ldots \quad \overline{x_n} = (x_n + c_n\overline{x_1})$$

tale che $f(\overline{x_1}, ..., \overline{x_n})$ è della forma $cx_1^N + \overline{f}$, con $deg_{x_1}(\overline{f}) < N$ e $c \neq 0$.

Dimostrazione. Esprimiamo f come somma di polinomi omogenei f_J di grado J: $f = f_N + ... + f_0$, con $f_N = A_{1,N}m_{1,N} + ... + A_{k_N,N}m_{k_N,N}$. Supponiamo che $m_{1,N}$ sia della forma X^α, con $\alpha = (a_1, ..., a_n)$. Se sostituiamo nel modo preannunciato otteniamo $f_N(\overline{x_1}, ..., \overline{x_n}) = f_N(1, c_2, ..., c_n)x_1^N +$ termini di grado inferiore ad N in x_1. Resta da soddisfare la richiesta che il coefficente di x_1^N sia diverso da zero. Poichè, però, il campo è algebricamente chiuso e infinito, e siamo in presenza di un polinomio, siamo sicuri di poter scegliere $c_2, ..., c_n$ tali che $f_n(1, c_2, ..., c_n) \neq 0$. □

Teorema 3.1. *Sia $\mathbb{K} = \overline{\mathbb{K}}$ e sia $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ ideale. Allora:*

- *(forma debole) $\mathbb{V}(I) = \emptyset \Leftrightarrow I = (1)$*
- *(forma forte) $\mathcal{I}(\mathbb{V}(I)) = \sqrt{I}$*

Dimostrazione. Dedichiamoci alla forma debole del teorema. É chiaro che $I = (1) \Rightarrow \mathbb{V}(I) = \emptyset$. Per quanto riguarda l'implicazione opposta, dimostriamola per induzione su n.

- *Passo Base*: $n = 1$, $I \subseteq \mathbb{K}[x]$. Se $I \neq (1) \Rightarrow I = (f(x))$, $degf > 0$. A questo punto il teorema fondamentale dell'algebra ci garantisce che $\mathbb{V}(I) \neq \emptyset$.
- *Passo Induttivo* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Ad $I_1 = I \cap \mathbb{K}[x_2, \ldots, x_n]$ si applica l'ipotesi induttiva. Se $I = I_1$ abbiamo finito, altrimenti scegliamo $f \in I - I_1 \mid deg(f, x_1) > 0$. Grazie al lemma precedente possiamo supporre che f sia della forma $f = cx_1^n + \ldots$. Per il Teorema di Estensione si ha $\pi : \mathbb{V}(I) \twoheadrightarrow \mathbb{V}(I_1)$; e poichè $\mathbb{V}(I) = \emptyset \Rightarrow \mathbb{V}(I_1) = \emptyset \Leftrightarrow 1 \in I_1 \Leftrightarrow 1 \in I$.

Passiamo adesso alla dimostrazione della forma forte. Faremo vedere le due inclusioni.

($\supseteq$) Sia $f \in \sqrt{I} \Leftrightarrow f^m \in I$. Dunque $\forall \alpha \in \mathbb{V}(I)\ f^m(\alpha) = (f(\alpha))^m = 0 \Rightarrow f(\alpha) = 0 \Leftrightarrow f \in \mathcal{I}(\mathbb{V}(I))$.

($\subseteq$) Sia $f \in \mathcal{I}(\mathbb{V}(I)) = \{g \in \mathbb{K}[x_1, \ldots, x_n] | \forall \alpha \in \mathbb{V}(I)\ g(\alpha) = 0\}$. Sia ora $J = (I, 1 - tf) \subseteq \mathbb{K}[x_1, \ldots, x_n, t]$. Abbiamo già mostrato la forma debole del teorema, dunque sappiamo che $\mathbb{V}(J) = \emptyset \Leftrightarrow 1 \in J$; il nostro obiettivo sarà mostrare che $\mathbb{V}(J) = \emptyset$. Supponiamo di avere $(\alpha_1, \ldots, \alpha_n, b) \in \mathbb{V}(J) \Rightarrow (\alpha_1, \ldots, \alpha_n) \in \mathbb{V}(I) \Rightarrow (1 - tf)(\alpha_1, \ldots, \alpha_n) = 1$, ovvero $\mathbb{V}(J) = \emptyset \Leftrightarrow 1 \in J$. Fissiamo dunque $g_1, \ldots, g_s$ generatori di I; possiamo scrivere

$$1 = \sum_{j=1}^{s} a_j(\underline{x}, t) g_j(\underline{x}) + h(\underline{x}, t)(1 - tf)(\underline{x}, t).$$

Valutiamo in $t = \frac{1}{f}$ e otteniamo

$$1 = \sum_{j=1}^{s} a_j(\underline{x}, \frac{1}{f}) g_j(\underline{x}) = \sum_{j=1}^{s} \frac{\overline{a}_j(\underline{x})}{f^{k_j}} g_j(\underline{x}).$$

Se $k = \max k_j \Rightarrow f^k = \sum_{j=1}^{s} \overline{a}_j(\underline{x}, t) g_j(\underline{x}) \Rightarrow f^k \in I \Leftrightarrow f \in \sqrt{I}$.

□

3.2 Dimensione di un Ideale

Introdurremo ora dei concetti che richiederebbero dei corsi interi per essere studiati in maniera appropriata.

Definizione 3.2.1. *La **dimensione** di Krull, o semplicemente dimensione, di un anello A è la massima lunghezza delle catene di primi distinti in A.*

Definizione 3.2.2. *Se $I \subseteq A$ è un ideale, ne definiamo la dimensione come la dimensione di Krull di A / I.*

Il concetto di dimensione presentato in questa maniera è molto astratto, e gli argomenti che affronteremo probabilmente non saranno di grande aiuto per acquisirvi familiarità. Questo, come anticipato, deriva dal fatto che servirebbe un intero corso solo per discutere lo studio della dimensione di un anello. Per noi sarà importante capire che $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ è **zero dimensionale** se riducendo per I otteniamo un insieme di resti i cui leading term sono in numero finito.

Se poi riflettiamo sul legame che vi è fra la base di Gröbner e la frontiera dell'ideale $LT(G) = LT(I)$, ci rendiamo conto che l'essere zero dimensionale equivale all'avere una frontiera minimale che interseca tutti gli assi coordinati.[1] Da questa riflessione la seguente proposizione.

Proposizione 3.2.1. *$I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Allora sono equivalenti:*

1. *$dim_{\mathbb{K}} \mathbb{K}[x_1, \ldots, x_n] \,/\, I < \infty$*
2. *$\forall i = 1, \cdots, n \; \exists h \in I \mid lm(h) = x_i^{s_i}$*
3. *Fissato un ordinamento, se $G = \{g_1, \cdots, g_k\}$ è una base di Gröbner $\Rightarrow \forall i = 1, \cdots, n \; \exists g_j \in G \mid lm(g_j) = x_i^{s_i}$*

Dimostrazione. Fissiamo un ordinamento e facendo vedere l'equivalenza tra 2) e 3).

3) $\Rightarrow$ 2) Segue banalmente dal fatto che i polinomi della base di Gröbner appartengano all'ideale.

2) $\Rightarrow$ 3) $\forall i = 1, ..., n$ possiamo scegliere $h \in I$ tale che $lm(h) = x_i^s$. G è base di Gröbner, quindi h riduce a 0 tramite G, da cui, in particolare, deduciamo che $\exists g_j \in G \mid lt(g_j) | lt(h) \Rightarrow lt(g_j) = x_i^m$, con $m \leq s_i$.

3) $\Rightarrow$ 1) Se $s_1, ..., s_n$ sono le minime potenze a cui compaiono le variabili x_i tra i leading monomial dei $g_j \in G$, allora, sicuramente, $\{x_1^{m_1} \cdots x_n^{m_n} \mid 0 \leq m_j \leq s_j \; \forall j = 1, ..., n\}$ è un sistema di generatori per $A \,/\, I$ nel senso che tutti i suoi elementi si possono ottenere come combinazioni a coefficenti in A di tali generatori.

1) $\Rightarrow$ 2) Dimostriamo la contronominale: se $\exists i \in \{1, ..., n\}$ tale che $\nexists h \in I$ il cui leading monomial è x_i^n per qualche $n \in \mathbb{N}$, allora per generare $A \,/\, I$ con combinazioni a coefficenti in A servono tutte le potenze di x_i, quindi la sua dimensione non può essere infinita.

□

[1] Sarebbe opportuno esplicitare i passaggi che permettono di stabilire questa equivalenza, ma ad ora non sono riuscita a farlo con gli strumenti garantiti da questo corso. Spero, a breve, di sopperire a questa mancanza. Sappiate che turba me almeno tanto quanto turba voi.

Proposizione 3.2.2. *Sia $\mathbb{K}$ algebricamente chiuso e $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. I è zero dimensionale $\Leftrightarrow \#\mathbb{V}(I) < \infty$.*

Dimostrazione. ($\Rightarrow$) Supponiamo che I sia 0 dimensionale e che la sua dimensione come spazio vettoriale su $\mathbb{K}$ sia N. Allora $\forall i = 1, ..., n1, x_i, ..., x_i^N$ sono linearmente dipendenti, quindi

$$\forall i \in 1, ..., n \ \exists b_{i,0}, ..., b_{i,N} \in \mathbb{K} \mid g_i(x_i) = \sum_{j=0}^{N} b_{i,j} x_i^j \equiv 0 \ mod(I)$$

da cui

$$(g_1, ..., g_n) \subseteq I \Rightarrow \mathbb{V}(g_1, ..., g_n) \supseteq \mathbb{V}(I)$$

Poichè ciascuno dei $g_i(x_i)$ ammette un numero finito di radici, deduciamo che $\mathbb{V}(I)$ deve essere finita.

($\Leftarrow$) Supponiamo ora $\#\mathbb{V}(I) < \infty$, ovvero $\mathbb{V}(I) = \{P_1, ..., P_k\}$, con $P_i = (a_1^i, ..., a_n^i)$ $\forall i = 1, ..., k$. Osserviamo allora che

$$\forall i = 1, ..., n \quad f_i(x_i) = \prod_{j=1}^{k} (x_i - a_i^j) \in \mathcal{I}(\mathbb{V}(I).$$

Poichè $\mathbb{K}$ è algebricamente chiuso, possiamo applicare il Nullstellensatz e affermare che $\forall i = 1, ..., n \ f_i(x_i) \in \mathcal{I}(\mathbb{V}(I)) = \sqrt{I} \Leftrightarrow \exists m_i \in \mathbb{N} \mid f_i(x_i) \in I$. Ma allora, poichè gli $f_i(x_i)$ sono monici nelle singole variabili x_i, abbiamo dimostrato che I è zero dimensionale.

□

3.3 Sistemi di Equazioni Polinomiali

In questa sezione cercheremo di dare ulteriore applicazione a quanto visto fino adesso. Ci occuperemo di sistemi di equazioni polinomiali: determineremo quando sono risolubili, se ammettono soluzioni finite, e vedremo in che modo è possibile ricondursi a situazioni analoghe a quelle dell'algebra linere per poterli risolvere.

Un sistema polinomiale è un sistema di equazioni della forma

$$\begin{cases} f_1(x_1, \cdots, x_n) = 0 \\ \cdots \\ f_k(x_1, \cdots, x_n) = 0 \end{cases}$$

Nel caso lineare, siamo abituati a portare il sistema in forma triangolare e poi a risolvere tramite sostituzione. Vorremmo fare qualcosa di simile, ma

vedremo che non sempre è possibile. Più precisamente, se $I = (f_1, \cdots, f_n) \subseteq \mathbb{K}[x_1, \ldots, x_n]$, $I_j = I \cap \mathbb{K}[x_{j+1}, \cdots, x_n]$, fissiamo l'ordinamento lessicografico con $x_1 > \cdots > x_n$, una base di Gröbner $G = \{g_1, \cdots, g_s\}$, e consideriamo la matrice

$$G = \begin{bmatrix} g_1^{(1)} & \cdots & \cdots & g_{s_1}^{(1)} \\ \cdots & g_1^{(2)} & \cdots & g_{s_2}^{(2)} \\ \cdots & & & \\ \cdots & & & \end{bmatrix}$$

dove la j-esima riga contiene gli elementi della base di Gröbner del j-esimo ideale di eliminazione.
Idealmente, vorremo definire un algoritmo di risoluzione analogo alla sostituzione all'indietro per sistemi triangolari superiori, ovvero vorremmo trovare soluzioni per l'i-esimo ideale di eliminazione e *sollevarle* all'(i-1)-esimo.
Vedremo, tuttavia, che questo è possibile solo sotto determinate ipotesi. Infatti, se abbiamo un sistema del tipo

$$\begin{cases} xz = 1 \\ xy = 1 \end{cases}$$

allora $I = (xz-1, xy-1)$ ha come base di Gröbner $G = \{xz-1, xy-1, z-y\}$ e come ideali di eliminazione i seguenti:

- $I_2 = I \cap \mathbb{K}[z] = (0) \Rightarrow \mathbb{V}(I_2) = \mathbb{V}((0)) = \mathbb{K}$;
- $I_1 = I \cap \mathbb{K}[y, z] = (y - z) \Rightarrow \mathbb{V}((I_1)) = \mathbb{V}((y - z)) = \{(a, a) \in \mathbb{K}^2 \mid a \in \mathbb{K}\}$;
- $I = (xz - 1, xy - 1, y - z) \Rightarrow \mathbb{V}(I) = \{(\frac{1}{a}, a, a) \mid a \neq 0, a \in \mathbb{K}\}$

É chiaro dal fatto che a debba essere diverso da zero che non tutte le soluzioni possano essere sollevate. Per dare una condizione sufficiente affinchè le soluzioni possano essere sollevate ci servirà il Risultante.

Definizione 3.3.1 (Risultante)**.** *Siano $f, g \in R[x]$, con R dominio. Se $f = \prod_{i=0}^{m} a_i x^i$ e $g = \prod_{i=0}^{m} b_i x_i$ allora si definisce Matrice di Sylvester di f e g la seguente*

$$Syl(f, g) = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & \cdots & \cdots & \cdots \\ \cdots & a_m & a_{m-1} & \cdots & a_0 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & \cdots & \cdots & \cdots \\ \cdots & b_n & b_{n-1} & \cdots & \cdots & b_0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & b_n & b_{n-1} & \cdots & b_0 \end{bmatrix}$$

Si tratta di una matrice $(n+m)\times(n+m)$, dove - precisiamo - le righe con i coefficenti di f sono n e quelle con i coefficenti di g sono m. Il suo determinante è quello che chiamiamo risultante di f e g.

Vedremo a breve svariate proprietà di questo oggetto; per ora, sfruttando quanto già sappiamo sul determinante, possiamo dire che:

1. $Ris(f,g)\in R$
2. $Ris(f,g)=(-1)^{nm}Ris(g,f)$
3. $Ris(af,g)=a^nRis(f,g), a\in R$
4. $Ris(a,f)=a^m, a\in R$
5. $Ris(a,b)=1, a,b\in R$

Osserviamo che il punto 4 deriva dal fatto che le costanti abbiano grado 0, quindi la matrice di Sylvester di f e a è aI. Invece, nel punto 5, si tratta di una convenzione.

É naturale chiedersi come si arrivi a studiare un oggetto come la matrice di Sylvester. La risposta sta nella seguente osservazione: supponiamo di voler trovare $A=d_{n-1}x^{n-1}+...+d_0$ e $B=c_{m-1}x^{m-1}+...+c_0$ polinomi in $R[x]$ tali che $Af+Bg=0$. Dalla scrittura $Af+Bg=0$ possiamo estrapolare $n+m$ equazioni lineari nei coefficenti c_j, d_j, ovvero le incognite, e la matrice relativa al sistema dato da tali equazioni è la trasposta adella matrice di Sylvester.
Perchè risolvere un tale sistema di equazioni? Perchè, come vedremo nel dettaglio a breve, ci dà informazioni sui fattori comuni ad f e g.

Prima di approcciarci a quelle proprietà del risultante che richiedono delle dimostrazioni più tecniche, introduciamo dei particolari polinomi.
Siano $z_1,\cdots,z_m$ indeterminate; denotiamo $f_m(x)=\prod_{j=1}^{m}(x-z_j)=\sum_{j=0}^{m}a_j^{(m)}x^j$, dove i coefficenti $a_j^{(m)}$ sono ottenuti applicando le funzioni elementari simmetriche alle indeterminate $z_1,\cdots,z_m$:

$$a_m^{(m)}=1$$

$$a_{m-1}^{(m)}=z_1+\cdots+z_m$$

$$a_{m-2}^{(m)}=z_1z_2+z_1z_3+\cdots+z_{m-1}z_m$$

$$\cdots$$

Osserviamo che i coefficenti sono lineari in ciascuna variabile e

$$f_{m-1}(x) = \frac{f_m(x)}{(x - z_m)} = \sum_{j=0}^{m-1} a_j^{(m-1)} x^j$$

poichè $a_{j-1}^{(m-1)}(z_1, \cdots, z_{m-1}) = a_j^{(m)}(z_1, \cdots, z_{m-1}, 0)$.

Detto ciò, possiamo enunciare e dimostrare il seguente

Lemma 3.3.1. *Sia* $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x], n \in \mathbb{N}, R$ *dominio. Allora* $Ris(f_m(x), g) = g(z_m) Ris(f_{m-1}, g)$.

Dimostrazione. Per dimostrare il lemma è necessario effettuare delle operazioni elementari sulla matrice di Sylvester associata a $f_m(x)$ e $g(x)$. Precisamente, osserviamo che se $\forall i = 1, ..., n + m$ *sommiamo all'ultima colonna la i-esima moltiplicata per* z_m^{m+n-i} l'ultima colonna diventa

$${}^t(z_m^{n-1} f_m(z_m), ..., f_m(z_m), z_m^{n-1} g(z_m), ..., g(z_m))$$

che è uguale a

$${}^t(0, ..., 0, z_m^{m-1} g(z_m), ..., g(z_m)).$$

Con queste operazioni non abbiamo modificato il determinante. Possiamo inoltre mettere in evidenza il fattore $g(z_m)$ e scrivere $det(Syl(f_m, g)) = g(z_m) det(Syl(f, g)')$, dove con $Syl(f, g)'$ intendiamo la matrice ottenuta dopo aver effettuato le varie operazioni descritte.
Osserviamo adesso che $g(z_m)$ è di grado n in z_m, così come $det(Syl(f, g))$, quindi $det(Syl(f, g)')$ non dipende da z_m. Allora poniamolo uguale a 0 all'interno della matrice e, calcolando il determinante con Laplace sull'ultima colonna, ora uguale a e_{m+n}, ottemiamo $det(Syl(f, g)) = g(z_m) det(Syl(f_{m-1}, g))$. □

Da questo risultato si deriva facilmente il seguente teorema.

Teorema 3.2. *Siano* $f(x) = \prod_{j=1}^{m} a_m(x - \alpha_j)$ *e* $g(x) = \prod_{j=1}^{n} b_n(x - \beta_j)$. *Allora valgono le seguenti proprietà:*

1. $Ris(f, g) = (-1)^{nm} b_n^m \prod_{j=1}^{n} f(\beta_j)$
2. $Ris(f, g) = a_m^n \prod_{j=1}^{m} g(\alpha_j)$
3. $Ris(f, g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$

Teorema 3.3. *Siano* $f, g \in R[x]$, *con* $f(x) = \sum_{j=0}^{m} a_j x^j$ *e* $g(x) = \sum_{j=0}^{n} b_j x^j$. *Allora* $\exists A, B \in R[x] \mid degA < n, degB < m$ *tali che*

$$Ris(f,g) = Af + Bg$$

da cui $Ris(f,g) \in R \cap (f,g))$

Dimostrazione. Come nel lemma precedente, moltiplichiamo la i-esima colonna di $Syl(f,g)$ per x^{m+n-i} e la sommiamo all'ultima colonna. Lo facciamo per ogni colonna, e infine otteniamo una matrice la cui ultima colonna è della forma

$$^t(x^{n-1}f(x), ..., xf(x), f(x), x^{m-1}g(x), ..., g(x))$$

Esclusa questa colonna, il resto della matrice è costante; se dunque ne calcoliamo il determinante con lo sviluppo di Laplace applicato all'ultima colonna otteniamo qualcosa del tipo

$$det(Syl(f,g)) = c_1 x^{n-1} f(x) + ... + c_n f(x) + d_1 x^{m-1} g(x) + ... + d_m g(x)$$

che è la combinazione polinomiale di f e g cercata. □

Proposizione 3.3.1. *Siano* f, g_1, g_2 *di gradi* m, n_1, n_2. *Allora*

$$Ris(f, g_1 g_2) = Ris(f, g_1) Ris(f, g_2).$$

Dimostrazione. Basta osservare che $\prod_j (g_1 g_2)(\alpha_j) = \prod_j (g_1)(\alpha_j) \prod_j (g_2)(\alpha_j)$, da cui

$$Ris(f, g_1 g_2) = a_m^{n_1+n_2} \prod (g_1 g_2)(\alpha_j) = a_m^{n_1} \prod_j g_1(\alpha_j) a_m^{n_2} \prod g_2(\alpha_j).$$

□

Proposizione 3.3.2. *Siano* f, g, h *polinomi, con* $deg(fh + g) = l$. *Allora*

$$Ris(f, fh + g) = a_m^{l-n} Ris(f, g),$$

con $n = deg(g)$.

Dimostrazione. Continuiamo a sfruttare le proprietà del risultante viste prima e osseviamo che

$$Ris(f, fh + g) = a_m^l \prod_j (fh + g)(\alpha_j) = a_m^{l-n} a_m^n \prod_j g(\alpha_j) = a_m^{l-n} Ris(f, g).$$

□

Il seguente teorema ci mostrerà un'altra importante proprietà del risultante, forse una delle più rilevanti.

Teorema 3.4. *Siano $f, g \in R[x]$ polinomi di grado maggiore di zero. f e g hanno un fattore comune di grado positivo $\Leftrightarrow Ris(f,g) = 0$.*

Dimostrazione. Deriva dalle prime proprietà che abbiamo enunciato. □

Con questi strumenti siamo pronti per dare una condizione sufficiente per il sollevamento di soluzioni di sistemi di equazioni polinomiali.

Teorema 3.5 (Teorema di Estensione)**.** *Sia $\mathbb{K} = \overline{\mathbb{K}}$, $I \subseteq \mathbb{K}[x_1, \ldots, x_n], I_1 = I \cap \mathbb{K}[x_2, \cdots, x_n]$. Consideriamo $I = (f_1, \cdots, f_n) \subseteq (\mathbb{K}[x_2, \cdots, x_n])[x_1]$, quindi $f_1 = g_{n_1}^{(1)}(x_2, \cdots, x_n)x_1^{n_1} + \overline{f_1}, deg(\overline{f_1}, x_1) < n_1$. Sia $\alpha \in \mathbb{V}(I_1)$. Se $\alpha \notin \mathbb{V}(g_{n_1}^{(1)}, \cdots, g_{n_k}^{(1)}) \Rightarrow \exists a \in \mathbb{K} \mid (a, \alpha) \in \mathbb{V}(I)$.*

Dimostrazione. Per semplicità, lo dimostriamo nel caso in cui $I = (f, g)$, ma tale dimostrazione si adatta con facilità al caso di n generatori.
Sia $I = (f, g)$, con $f = a_m(x_2, ..., x_n)x_1^m + ...$ e $g = b_s(x_2, ..., x_n)x_1^s + ...$, dove i termini omessi sono tutti di grado inferiore nella variabile x_1. Osserviamo che $Ris_{x_1}(f, g) \in \mathbb{K}[x_2, ..., x_n] \cap I = I_1$, dunque $Ris_{x_1}(f, g) = H(x_2, ..., x_n)$. Sia ora $\alpha \in \mathbb{V}(I_1)$. Sicuramente $H(\alpha) = 0$, a noi però interessa che $H(x_2, ..., x_n) = Ris(f(x_1, \alpha), g(x_1, \alpha))$, ovvero che la valutazione e il calcolo del risultante commutino. Affinchè tale richiesta sia soddisfatta, è sufficiente che la matrice non cambi dimensione, quindi che i gradi di f e g rimangano invariati. Per ipotesi, abbiamo che α *non* è radice sia di $a_m(x_2, ..., x_n)$ che di $b_s(x_2, ..., x_n)$, quindi possiamo supporre che $a_m(\alpha) \neq 0$. Allora concludiamo osservando che scegliendo $N > deg(g, x_1)$, $lc(x_1 N f + g) = a_m$, quindi la valutazione in α e il calcolo di $Ris(f, x_1^N f + g)$ commutano. Arrivati a questo punto, possiamo dire di aver concluso perchè $H(x_2, ..., x_n) = Ris(f, x_1^N f + g) = Ris(f, g)$ valutato in α fa 0, quindi possiamo risolvere per x_1 e sollevare α. □

3.4 Topologia di Zariski

Introduciamo adesso una topologia su $\mathbb{K}^n$ e su $Spec(A)$, con A anello commutativo con unità.

Per quanto riguarda $\mathbb{K}^n$, se $S \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é un qualsiasi sottoinsieme, un chiuso nella Topologia di Zariski su $\mathbb{K}^n$ è un insieme della forma:

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

Questi sottoinsiemi definiscono effettivamente una topologia poichè

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

quindi l'unione finita di chiusi è ancora un chiuso, e l'intersezione qualsiasi di chiusi è ancora un chiuso.

In altri termini, ci siamo resi conto che le varietà affini in $\mathbb{K}^n$ sono i chiusi di una topologia. Tuttavia, non ogni sottoinsieme di $\mathbb{K}^n$ è una varietà - per convincersene basta considerare $\mathbb{K} - \{0\}$[2]. Dato allora un generico $S \subseteq \mathbb{K}^n$ consideriamo

$$\mathcal{I}(S) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(\alpha) = 0 \ \forall \alpha \in S\}$$

Questo insieme è un ideale radicale in $\mathbb{K}[x_1, \ldots, x_n]$, e a lui è associata la varietà $\mathbb{V}(\mathcal{I}(S))$. Con il seguente lemma vogliamo dimostrare che $\mathbb{V}(\mathcal{I}(S))$ è la più piccola varietà che contiene S.

Lemma 3.4.1. *Se $S \subseteq \mathbb{K}^n$ è un generico sottoinsieme, $\mathbb{V}(\mathcal{I}(S))$ è la più piccola varietà che contiene S.*

Dimostrazione. In primo luogo osserviamo che $\mathbb{V}(\mathcal{I}(S))$ è sicuramente una varietà in quanto $\mathcal{I}(S)$ è un ideale $\Rightarrow$ è un chiuso nella topologia di Zariski su $\mathbb{K}^n$. Sia ora W una varietà che contiene S.

$$W \supseteq S \Rightarrow \mathcal{I}(W) \subseteq \mathcal{I}(S) \Rightarrow \mathbb{V}(\mathcal{I}(W)) \supseteq \mathbb{V}(\mathcal{I}(S))$$

ma W è una varietà $\Rightarrow \mathbb{V}(\mathcal{I}(W)) = W \Rightarrow W \supseteq \mathbb{V}(\mathcal{I}(S))$. □

Definizione 3.4.1 (Chiusura di un sottoinsieme di $\mathbb{K}^n$)**.** *Sia S un generico sottoinsieme di $\mathbb{K}^n$, sul quale consideriamo la topologia di Zariski. Definiamo* ***chiusura di Zariski*** *di S, e la denotiamo con $\overline{S}$, la più piccola varietà affine che contiene S.*

Il lemma appena dimostrato ci dice che $\overline{S} = \mathbb{V}(\mathcal{I}(S))$.

Legheremo ora, grazie anche alla topologia di Zariski, la varietà del colon di due ideali con la differenza di varietà.

Proposizione 3.4.1. *Siano $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$. In generale si ha che $\mathbb{V}(I : J) \supseteq \overline{\mathbb{V}(I) - \mathbb{V}(J)}$; se però $\mathbb{K} = \overline{\mathbb{K}}$ e $I = \sqrt{I} \Rightarrow \mathbb{V}(I : J) = \overline{\mathbb{V}(I) - \mathbb{V}(J)}$.*

[2]Effettivamente, poichè su $\mathbb{K}$ i chiusi sono i luoghi di zeri di polinomi in una variabile, è facile capire che sottoinsiemi infiniti non possono essere chiusi. Questo ci fa anche osservare che la topologia di Zariski su $\mathbb{K}$ è la topologia cofinita

Dimostrazione. Per convincerci che $\mathbb{V}(I:J) \supseteq \overline{\mathbb{V}(I) - \mathbb{V}(J)} = \mathbb{V}(\mathcal{I}(\mathbb{V}(I) - \mathbb{V}(J)))$ mostriamo che $(I:J) \subseteq \mathcal{I}(\mathbb{V}(I) - \mathbb{V}(J))$.

$$f \in (I:J) \Rightarrow \forall g \in J \ fg \in I \Rightarrow \forall \alpha \in \mathbb{V}(I) - \mathbb{V}(J) \ fg(\alpha) = f(\alpha)g(\alpha) = 0.$$

Ora, poichè $\alpha \in \mathbb{V}(I) - \mathbb{V}(J)$ possiamo scegliere g come uno di quei polinomi di J che non si annulla in $\alpha \Rightarrow f(\alpha) = 0$. Applicando la mappa $\mathbb{V}$ abbiamo la prima inclusione.
Per l'altra inclusione facciamo di nuovo vedere l'inclusione opposta fra gli ideali: $\mathbb{V}(I:J) \subseteq \overline{\mathbb{V}(I) - \mathbb{V}(J)} \Leftarrow (I:J) \supseteq \mathcal{I}(\mathbb{V}(I) - \mathbb{V}(J))$. Sia dunque $h \in \mathcal{I}(\mathbb{V}(I) - \mathbb{V}(J))$ e sia $g \in J$; vogliamo far vedere che $hg \in I$. Abbiamo ora però delle ipotesi in più: $\mathbb{K} = \overline{\mathbb{K}}$ e $I = \sqrt{I}$, quindi possiamo applicare il Nullstellensatz e affermare che $I = \sqrt{I} = \mathcal{I}(\mathbb{V}(I))$. La tesi è quindi equivalente a $hg \in \mathcal{I}(\mathbb{V}(I))$.
Sia dunque $\alpha \in \mathbb{V}(I)$. É del tutto lecito scrivere che $\mathbb{V}(I) = (\mathbb{V}(I) - \mathbb{V}(J)) \cup (\mathbb{V}(I) \cap \mathbb{V}(J))$, da cui $\alpha \in \mathbb{V}(I) - \mathbb{V}(J) \Rightarrow h(\alpha)g(\alpha) = 0g(\alpha) = 0$, altrimenti $\alpha \in \mathbb{V}(I) \cap \mathbb{V}(J) \Rightarrow h(\alpha)g(\alpha) = h(\alpha)0 = 0$. In conclusione $hg \in \mathcal{I}(\mathbb{V}(I))$. □

Ora che disponiamo di questi strumenti topologici, riapriamo la questione del sollevamento di soluzioni per sistemi di equazioni polinomiali.
Sia $\mathbb{V}(I) \subseteq \mathbb{K}^n$, dove $I = (f_1, \cdots, f_s) \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Consideriamo la mappa di proiezione

$$\begin{aligned} \pi_l : \mathbb{K}^n &\longrightarrow \mathbb{K}^{n-l} \\ (a_1, \cdots, a_n) &\mapsto (a_{l+1}, \cdots, a_n) \end{aligned}$$

dove $\mathbb{K}^{n-l} \cong \mathbb{K}[x_{l+1}, \cdots, x_n] \supseteq I_l$.
Ci chiediamo che relazione vi sia tra $\pi_l(\mathbb{V}(I))$ e $\mathbb{V}(I_l)$. In generale vale il contenimento $\pi_l(\mathbb{V}(I)) \subseteq \mathbb{V}(I_l)$, infatti se

$$P \in \pi_l(\mathbb{V}(I)) \text{ e } f \in I_l \Leftrightarrow f = \sum_{i=1}^{s} \alpha_i f_i, \ f_i \in \mathbb{K}[x_{l+1}, \cdots, x_n]$$

allora

$$f(P) = f(a_1, \cdots, a_n) = f(a_{l+1}, \cdots, a_n) = 0 \Leftrightarrow \forall \alpha \in \mathbb{V}(I) \ f(\pi_l(\alpha)) = 0.$$

Se però il campo su cui lavoriamo è algebricamente chiuso riusciamo a dimostrare l'esistenza di un più forte legame tra i due oggetti.

Teorema 3.6 (The Closure Theorem)**.** *Nelle notazioni adottate fino ad adesso, si ha:* $\mathbb{K} = \overline{\mathbb{K}} \Rightarrow \overline{\pi_l(\mathbb{V}(I))} = \mathbb{V}(I_l)$.

Dimostrazione. In generale $\pi_l(\mathbb{V}(I)) \subseteq \mathbb{V}(I_l) \Rightarrow \mathcal{I}(\pi_l(\mathbb{V}(I)) \supseteq \mathcal{I}(\mathbb{V}(I_l)) \Rightarrow \mathbb{V}(idv(\pi_l(\mathbb{V}(I)))) \subseteq \mathbb{V}(I_l)$. Per l'altra inclusione consideriamo $f \in \mathcal{I}(\pi_l(\mathbb{V}(I))) \Rightarrow \forall \alpha \in \mathbb{V}(I)\ f(\pi_l(\alpha)) = 0$. Poichè, evidentemente, f non dipende dalle prima l variabili, possiamo affermare che $\forall \alpha \in \mathbb{V}(I)\ f(\alpha) = 0 \Leftrightarrow f \in \mathcal{I}(\mathbb{V}(I))$; ma $\mathbb{K}$ è algebricamente chiuso, quindi il Nullstellensatz ci dice che $f \in \sqrt{I} \Leftrightarrow \exists N \in \mathbb{N} \mid f^N \in I$. D'altra parte, appunto per il fatto che f non dipende dalle prime l variabili, si ha che $f^N \in I_l \Leftrightarrow f \in \sqrt{I_l}$. Ma avevamo scelto f in $\mathcal{I}(\pi_l(\mathbb{V}(I))) \Rightarrow$ abbiamo mostrato che $\mathcal{I}(\pi_l(\mathbb{V}(I))) \subseteq \sqrt{I_l} = \mathcal{I}(\mathbb{V}(I_l)) \Rightarrow \mathbb{V}\mathcal{I}(\pi_l(\mathbb{V}(I))) \supseteq \mathbb{V}(\mathcal{I}(\mathbb{V}(I_l))) = \mathbb{V}(I_l)$. □

Un'altra topologia che è per noi di particolare interesse è la Topologia di Zariski sullo Spettro di un Anello. Consideriamo un generico anello A con unità, il suo insieme di ideali primi $Spec(A)$, ed un suo generico sottoinsieme $E \subseteq A$.

Proposizione 3.4.2 (Topologia di Zariski su $Spec(A)$)**.** *Gli insiemi* $\mathbb{V}(E) = \{\mathfrak{p} \in Spec(A) | E \subseteq \mathfrak{p}\}$ *sono i chiusi di una topologia su* $Spec(A)$*, infatti:*

1. $\mathbb{V}(E) = \mathbb{V}((E)) = \mathbb{V}(\sqrt{(E)})$
2. $\mathbb{V}((0)) = Spec(A)$
3. $\mathbb{V}((1)) = \emptyset$
4. *Se* $(E_j)_{j\in J}$ *è una famiglia di sottoinsiemi, allora* $\mathbb{V}\left(\bigcup_{j\in J} E_j\right) = \bigcap_{j\in J} \mathbb{V}(E_j)$
5. $\mathbb{V}(I \cap J) = \mathbb{V}(IJ) = \mathbb{V}(I) \cup \mathbb{V}(J)$*, con* $I, J \subseteq A$ *ideali*

Dimostrazione.

1. Segue dalla definizione di ideale che se $\mathfrak{p} \supseteq E \Rightarrow \mathfrak{p} \supseteq (E)$. Segue invece dalla definizione di ideale primo che $\mathfrak{p} \supseteq (E) \Leftrightarrow \mathfrak{p} \supseteq \sqrt{(E)}$.
2. $\mathbb{V}((0)) = \{\mathfrak{p} \in Spec(A) \mid \mathfrak{p} \supseteq (0)\}$, ma lo 0 è contenuto in ogni ideale $\Rightarrow \mathbb{V}((0)) = Spec(A)$.
3. Gli ideali primi, per definzione, sono ideale propri, quindi non possono contenere $(1) = A$, da cui $\mathbb{V}((1)) = \emptyset$.
4. $\mathfrak{p} \in \bigcap_{j\in J} \mathbb{V}(E_j) \Leftrightarrow \mathfrak{p} \supseteq E_j\ \forall j \in J \Leftrightarrow \mathfrak{p} \supseteq \bigcup_{j\in J} E_j \Leftrightarrow \mathfrak{p} \in \mathbb{V}\left(\bigcup_{j\in J} E_j\right)$.
5. $\mathfrak{p} \in \mathbb{V}(I \cap J) \Leftrightarrow \mathfrak{p} \supseteq I \cap J \Leftrightarrow \mathfrak{p} \supseteq I \wedge \mathfrak{p} \supseteq J \Leftrightarrow \mathfrak{p} \in \mathbb{V}(I \cup J)$. Ma se $\mathfrak{p} \supseteq I \vee \mathfrak{p} \supseteq J \Rightarrow \mathfrak{p} \supseteq IJ \Rightarrow \mathfrak{p} \subseteq I \cap J$, ovvero $\mathbb{V}(I) \cup \mathbb{V}(J) \subseteq \mathbb{V}(IJ) \subseteq \mathbb{V}(I \cap J)$, da cui l'uguaglianza.

□

Ora che disponiamo di questi strumenti topologici, introduciamo due nuovi concetti.

Definizione 3.4.2. *Una varietà* $\mathbb{V}$ *si dice irriducibile se* $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2$*, con* $\mathbb{V}_1$ *e* $\mathbb{V}_2$ *varietà, allora* $\mathbb{V} = \mathbb{V}_1 \vee \mathbb{V} = \mathbb{V}_2$.

Analogamente:

Definizione 3.4.3. *Un ideale* I *di un anello* A *si dice irriducibile se* $I = I_1 \cap I_2$*, con* I_1, I_2 *ideali, allora* $I = I_1 \vee I = I_2$.

Iniziamo a legare queste definizioni con altre nozioni già viste.

Proposizione 3.4.3. *Sia* $\mathbb{V}$ *una varietà. Allora* $\mathbb{V}$ *è irriducibile* $\Leftrightarrow$ $\mathcal{I}(\mathbb{V})$ *è primo*

Dimostrazione. Dimostriamo le due implicazioni.

($\Rightarrow$) Sia $\mathbb{V}$ irriducibile e sia $fg \in \mathcal{I}(\mathbb{V})$. Allora, se poniamo $\mathbb{V}_1 = \mathbb{V} \cap \mathbb{V}(f)$ e $\mathbb{V}_2 = \mathbb{V} \cap \mathbb{V}(g)$, segue che $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2$. Ma $\mathbb{V}$ è irriducibile $\Rightarrow \mathbb{V} = \mathbb{V}_1 \vee \mathbb{V} = \mathbb{V}_2$. Senza perdità di generalità, supponiamo che valga $\mathbb{V} = \mathbb{V} \cap \mathbb{V}(f) \Rightarrow$ f si annulla su tutti gli elementi di $\mathbb{V} \Leftrightarrow f \in \mathcal{I}(\mathbb{V}) \Rightarrow \mathcal{I}(\mathbb{V})$ è primo.

($\Leftarrow$) Sia $\mathcal{I}(\mathbb{V})$ primo e sia $\mathbb{V} = \mathbb{V}_1 \cup \mathbb{V}_2$. Supponiamo $\mathbb{V}_1 \subsetneq \mathbb{V} \Rightarrow \mathcal{I}(\mathbb{V}_1) \supsetneq \mathcal{I}(\mathbb{V})$. Vogliamo dimostrare che $\mathbb{V} = \mathbb{V}_2$; per farlo verificheremo l'uguaglianza tra i rispettivi ideali. Sappiamo già che $\mathbb{V}_2 \subseteq \mathbb{V} \Rightarrow \mathcal{I}(\mathbb{V}_2) \supseteq \mathcal{I}(\mathbb{V})$. Siano ora $g \in \mathcal{I}(\mathbb{V}_2)$ e $f \in \mathcal{I}(\mathbb{V}_1) - \mathcal{I}(\mathbb{V})$. $fg \in \mathcal{I}(\mathbb{V}_1) \cap \mathcal{I}(\mathbb{V}_2) \Rightarrow fg \in \mathcal{I}(\mathbb{V})$. Ma allora, poichè $f \notin \mathcal{I}(\mathbb{V})$ segue che $g \in \mathcal{I}(\mathbb{V})$, da cui l'altra inclusione.

□

Osservazione. Se $\mathbb{V}$ è una varietà irriducibile $\Rightarrow \exists\ \mathfrak{p} \in Spec(\mathbb{K}[x_1, \ldots, x_n])$ tale che $\mathbb{V} = \mathbb{V}(\mathfrak{p})$. Non è vero il viceversa! Consideriamo infatti $(x + y) \subseteq (\mathbb{Z}/(2))[x, y]$. I è primo poichè $(\mathbb{Z}/(2))[x, y]/I \cong (\mathbb{Z}/(2))[x]$ è integro, ma $\mathbb{V}(I) = \{(0, 0), (1, 1)\} = \{(0, 0\} \cup \{(1, 1)\}$. Questo controesempio esiste perchè $\mathbb{Z}/(2)$ non è algebricamente chiuso!

Capitolo 4

Moduli

Introduciamo ora la struttura di *modulo*, grazie alla quale riusciremo a generalizzare la struttura di spazio vettoriale

Definizione 4.0.1. *Sia A un anello con identità ed M un insieme. Diremo che M è un A-modulo se valgono le seguenti proprietà:*

1. *$(M, +)$ è un gruppo abeliano;*
2. *Esiste un prodotto esterno del tipo*

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto am \end{aligned}$$

tale che $\forall a, b \in A$, $\forall m \in M$:

   (a) $(a + b)m = am + bm$
   (b) $a(m + n) = am + an$
   (c) $a(bm) = (ab)m$
   (d) $1 \cdot m = m$

Osservazione. I due zeri $0_A, 0_B$ verificano $0_A \cdot m = 0_M$, $a \cdot 0_m = 0_M$.

In che senso, dunque, stiamo generalizzando la teoria degli spazi vettoriali? La risposta sta in quest'altra osservazione: *se scegliamo $A = \mathbb{K}$ campo, allora A-modulo $\Leftrightarrow \mathbb{K}$ spazio vettoriale.*
É inoltre lecito considerare $A = M$, e dunque A come A-modulo su se stesso, oppure $B \subseteq A$ sottoanello ed A come B-modulo. Se invece $A = \mathbb{Z}$, è interessante osservare che *gli $\mathbb{Z}$ moduli sono i gruppi abeliani.*

4.1 Sottomoduli

Consideriamo $N \subseteq M$ sottoinsieme di M A-modulo. Diremo che N è un sottomodulo se $N < M$ e $\forall a \in A, \forall n \in N\ an \in N$.
Se consideriamo A come A-modulo, i suoi sottomoduli sono gli ideali. Proviamo dunque a definirvi delle operazioni.

Definizione 4.1.1. *$I \in A$ ideale. $IM = \{\sum_{j=1}^{k} a_j m_j | a_j \in A, m_j \in m\} \subseteq M$ è un sottomodulo per definizione di ideale.*

Definizione 4.1.2. *Sia $S \subseteq M$ sottoinsieme. Il sottomodulo[1] generato da S, $< S >= \{\sum_{j=1}^{k} |a_j s_j | a_j \in A, s_j \in S\}$, è il più piccolo sottomodulo contenente S. Diremo dunque che S è un **insieme di generatori** se $< S >= M$, e se $|S| < \infty$ diremo che M è finitamente generato.*

Il concetto di lineare indipendenza assume invece questa forma:

Definizione 4.1.3. *$S \subseteq M$ sottoinsieme è **libero** se $\sum_{j=1}^{k} a_j s_j = 0 \Rightarrow a_j = 0\ \forall j \in \{1, \dots, k\}$*

e quello di base, come ci si aspetta, è il seguente:

Definizione 4.1.4. *Un sottoinsieme S è una base di M, A-modulo, se è libero e genera.*

Definizione 4.1.5. *Un A-modulo si dice **libero** se ammette una base.*

Sorge spontanea la seguente domanda: *in quali casi possiamo dire con certezza che un modulo ammette una base?* Una provvisoria risposta ci è data dai seguenti esempi: A ed $A \times \cdots \times A$ come A-moduli. Possiamo infatti scegliere come basi, rispettivamente, $\{1\}$ e l'insieme dei vettori coordinati. Un esempio di modulo *non* libero, invece, ci è invece dato da $\mathbb{Q}$ visto come $\mathbb{Z}$-modulo.
Enunciamo ora una proposizione in grado di dissolvere alcuni dei dubbi che ad ora dovremmo aver sviluppato.

Proposizione 4.1.1. *Se M è un A-modulo libero finitamente generato, allora tutte le basi hanno medesima cardinalità. Tale cardinalità è detta **rango**.*

Dimostrazione. Sia $B = \{m_1, \cdots, m_j\}$ base per M e sia $I \subseteq A$ ideale massimale. M/IM è un $A\,/\,I$-modulo, ma I *massimale* $\Leftrightarrow A\,/\,I$ *campo* quindi $M\,/\,IM$ è uno spazio vettoriale. Consideriamo ora la mappa di proiezione: $\pi : M \twoheadrightarrow M\,/\,IM \mid m_j \longmapsto \overline{m_j}$. Sicuramente gli $\{\overline{m_j}\}$ generano; se facciamo

[1] Verificatelo!

vedere che sono anche linearmente indipendenti abbiamo mostrato che tutte le basi finite hanno medesima cardinalità. Sia allora

$$\sum_{j=1}^{k} \overline{a_j m_j} \equiv 0 \Leftrightarrow \sum_{j=1}^{k} a_j m_j \in IM$$

ma B è una base, dunque $\sum\limits_{j=1}^{k} a_j m_j = \sum\limits_{j=1}^{k} b_j m_j$, con $b_j \in I$, da cui

$$\sum_{j=1}^{k} (a_j - b_j) m_j = 0 \Leftrightarrow \sum_{j=1}^{k} (\overline{a_j - b_j}) \overline{m_j} \equiv 0$$

da cui $\forall j = 1, ..., k \quad \overline{a_j} \equiv \overline{b_j} \equiv 0$. □

Non affronteremo il caso in cui il modulo è libero ma non finitamente generato, a ogni modo possiamo osservare che se C fosse una base infinita per M, allora $\forall j = 1, \cdots, k$ avremmo che $m_j = \sum\limits_{i=1}^{t_j} a_i n_{ij}$, con $n_{ij} \in C$. Ma allora l'insieme di tutti gli n_{ij} è un sottoinsieme di C che genera M $\Rightarrow \forall h \in C - \{n_{ij}\} \mid h = \sum d_j m_j = \sum d_{ij} n_{ij}$, che è assurdo perchè abbiamo supposto che C fosse una base.
Con maggiore attenzione ai dettagli, si può arrivare a dimostrare che se un modulo ammette una base infinita, allora non ne ammette di finite.

Osservazione. Se M è un modulo libero finitamente generato ogni insieme di generatori ha cardinalità maggiore o uguale al rango.

Proposizione 4.1.2. *Siano $N, M_1, M_2 \subseteq M$ sottomoduli. Allora*

$$Ann(M / N) = (N : M)$$

dove $(N : M) = \{a \in A \mid aM \subseteq N\}$, e $Ann(M_1 + M_2) = Ann(M_1) \cap Ann(M_2)$.

Dimostrazione. Per quanto riguarda il primo enunciato, osserviamo che $a \in Ann(M / N) = (0 : M / N)$, dunque $a(b + N) = N \Leftrightarrow ab \in N \Leftrightarrow a \in (N : M)$.
Per il secondo punto, comunciamo osservando che $M_1, M_1 \subseteq M_1 + M_2 \Rightarrow Ann(M_1 + M_2) \subseteq Ann(M_1) \cap Ann(M_2)$. D'altra parte, se $aM_1 = aM_2 = 0 \Rightarrow a(M_1 + M_2) = 0$. □

4.2 Omomorfismi di Moduli

Un omomorfismo f di A-moduli è un omomorfismo di gruppi A-lineare, ovvero $f(m+n) = f(m) + f(n)$ e $f(am) = af(m)$ $\forall m, n \in M$ $\forall a \in A$. Osserviamo che *non* stiamo imponendo $1_M \longmapsto 1_N$, dunque abbiamo più libertà quando definiamo omomorfismi tra A moduli. Un esempio ci è dato da $\mathbb{Z}$, il cui unico omomorfismo come anello è l'identità, che ammette però vari omomorfismi come $\mathbb{Z}$-modulo, ad esempio $f : 1 \longmapsto 2$.
Definiamo poi $Hom_A(M, N) := \{f : M \to N | f$ omomorfismo di A moduli$\}$ e lo dotiamo delle seguenti operazioni, che lo renderanno un A-modulo:

$(+)$ $\forall f, g \in Hom_A(M, N), (f + g)(m) = f(m) + g(m)$

$(\cdot)$ $\forall f \in Hom_A(M, N), \forall a \in A, af(m) = f(am)$

Sia ora $f \in Hom_A(M, N)$. Si verifica che $Kerf \subseteq M$ è sottomodulo di M e $Imf \subseteq N$ è sottomodulo di N, infatti:

> $(Kerf)$ $\forall m, n \in kerf, \forall a \in A, 0 = 0+0 = f(m)+f(n) = f(m+n) = 0$ e $af(m) = a \cdot 0 = 0$
>
> (Imf) $\forall f(m), f(n) \in Imf, \forall a \in A, f(m)+f(n) = f(m+n)$ e $af(m) = f(am)$

Vorremo inoltre che fosse ben definito $cokerf := N \,/\, Imf$, quindi soffermiamoci sui quozienti.
Se $N \subseteq M$ è un sottomodulo, $M \,/\, N$ è un A-modulo con le seguenti operazioni:

> $(+)$ trattandosi di gruppi abeliani, $M \,/\, N$ è gruppo abeliano;
>
> $(\cdot)$ $\forall a \in A, a(m + N) = am + N$ poichè se $m + N = m + n + M \Rightarrow a(m + n + N) = am + an + N = am + N$, in quanto $n \in N$.

Continuano a valere i Teoremi di Omomorfismo.

Teorema 4.1 (I Teorema di Omomorfismo)**.** *M, N A-moduli, $f \in Hom_A(M, N)$. Allora vale $Imf \cong M \,/\, Kerf$.*

Teorema 4.2 (II Teorema di Omomorfismo)**.** *$P \supseteq M \supseteq N$ A-moduli. Allora vale $P \,/\, M \cong (P \,/\, N)/(M \,/\, N)$.*

Dimostrazione. Si dimostra applicando il Primo Teorema di Omomorfismo alla mappa $\pi : P \,/\, N \twoheadrightarrow P \,/\, M$. □

Esercizio. Sia M un A-modulo. Allora $Hom_A(A, M) \cong M$ tramite la mappa $m \in M \longmapsto f_m \in Hom_A(A, M)$, dove $\forall m \in M$ $f_m : 1 \longmapsto m$.

Esercizio. $Hom_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = \{0\}$ poichè $\forall \phi \in Hom_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z})$ si ha $\phi(1) = \phi(\frac{p}{p}) = p\phi(\frac{1}{p}) \Rightarrow p|\phi(1)\ \forall p$ primo in $\mathbb{Z}$, che è assurdo a meno che $\phi(1) = 0$.

Esercizio. $Hom_{\mathbb{Z}}(\mathbb{Z}/(2)),\mathbb{Z}) = \{0\}$ poichè $\forall \phi \in Hom_{\mathbb{Z}}(\mathbb{Z}/(2))\ \phi(0) = 0 = \phi(2m) = 2\phi(m) \Rightarrow \phi(m) = 0\ \forall m \in \mathbb{Z}/(2)$.

Invece...

Esercizio. $Hom_{\mathbb{Z}}(\mathbb{Z}/(2),\mathbb{Q}/\mathbb{Z}) \neq \{0\}$ poichè è ben definito $\phi : 1 \longmapsto \frac{1}{2} + \mathbb{Q}/\mathbb{Z}$.

Esercizio. $Hom_{\mathbb{Z}}(\mathbb{Z}/(m),\mathbb{Z}/(n)) \cong \mathbb{Z}/(m,n)$.

Torniamo ora agli ideali e al loro legame con i sottomoduli. In particolare, vediamo fino a che punto sono analoghi gli uni agli altri dal punto di vista delle operazioni.

Definizione 4.2.1 (Somma di Sottomoduli)**.** *Siano $M_1, M_2 \subseteq M$ sottomoduli. Allora definiamo $M_1 + M_2 = \{m_1 + m_2 | m_1 \in M_1, m_2 \in M_2\}$.*

Più in generale, se abbiamo una famiglia $\{M_j\}_{j\in J}$ definiamo

$$\sum_{j\in J} M_J := \{\sum_{j\in J}^{k} m_j | m_j \in M_j, k \in \mathbb{N}\}.$$

Osserviamo poi che l'intersezione è un sottomodulo, mentre, in generale, $(M_1 : M_2) = \{a \in A | aM_2 \subseteq M_1\}$ è un ideale ma *non* è un sottomodulo. Ricordiamo, in particolare, $(0 : M) = Ann(M)$, il quale tornerà prossimamente ad essere al centro della nostra attenzione.

Proposizione 4.2.1. *Siano $M_1, M_2 \subseteq M$ sottomoduli di un A-modulo. Allora $M_1 + M_2 / M_1 \cong M_2 / M_1 \cap M_2$.*

Dimostrazione. Consideriamo la composizione delle seguenti mappe di inclusione e proiezione: $M_2 \hookrightarrow M_1 + M_2 \twoheadrightarrow M_1 + M_2 / M_1$. Ci chiediamo chi sia il nucleo della loro composizione. Se $\overline{m_2}$ è un elemento nell'immagine, allora $\overline{m_2} \equiv 0 \Leftrightarrow m_2 \in M_1 \Leftrightarrow m_2 \in M_1 \cap M_2$, quindi abbiamo la tesi dal Primo Teorema di Omomorfismo. □

4.3 Somma Diretta

Data una famiglia $\{M_i\}_{i\in H}$ di A-moduli, con H famiglia arbitraria di indici, vorremmo definire tra loro la struttura di somma diretta. Come varie altre volte in passato, la somma diretta ci sarà utile per dimostrare teoremi di struttura.

Definizione 4.3.1. *Siano M_1, M_2 due A-moduli. Definiamo somma diretta l'insieme $M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}$.*

Se definiamo le operazioni componente per componente, la somma diretta può essere vista anch'essa come A-modulo.
Estendiamo ora questa definizione ad una famiglia qualsiasi di moduli, purchè siano moduli sul medesimo anello.

Definizione 4.3.2. *Data una famiglia di A-moduli $\{M_i\}_{i\in H}$ con H famiglia arbitraria di indici, definiamo somma diretta l'insieme*

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

Se eliminiamo la richiesta che vi sia un numero finito di componenti diverse da zero, allora si parla di prodotto diretto.

Definizione 4.3.3. *Data una famiglia di A-moduli $\{M_i\}_{i\in H}$ con H famiglia arbitraria di indici, definiamo prodotto diretto l'insieme*

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

Chiaramente se $\#H < \infty$ somma diretta e prodotto diretto coincidono.

Come anticipato, ecco un primo risultato di struttura.

Proposizione 4.3.1. *Sia M un A-modulo libero. Allora*

$$M \cong \bigoplus_{i\in H} M_i,\ M_i \cong A\ \forall i \in H$$

ovvero M è isomorfo alla somma diretta di moduli ciclici, ognuno dei quali è naturalmente isomorfo all'anello A.

Dimostrazione. Sia M libero e sia $B = \{b_i\}_{i\in H}$ una sua base. Allora

$$\forall m \in M,\ m = \sum_{i=1}^{k} a_i b_i, a_i \in M \quad \forall i = 1, ..., k$$

da cui la mappa surgettiva

$$\begin{aligned} \phi : M &\longrightarrow \bigoplus_{i\in H} A \\ b_i &\longmapsto e_i \end{aligned}$$

Osserviamo che ha senso parlare di somma diretta perchè nonostante H non sia necessariamente finito, sappiamo che, per definizione, B è base perchè tutti gli elementi di M possono essere ottenuti come combinazione *finita* di elementi di B a coefficenti in A .
Ciò detto, ϕ è un isomorfismo per lineare indipendenza degli elementi della base:

$$\text{se } m = \sum_{i \in H} a_i b_i \text{ e } \phi(m) = 0 \Rightarrow \sum_{i \in H} a_i b_i = 0 \Leftrightarrow a_i = 0 \ \forall i \in H.$$

Dal Primo Teorema di Omomorfismo abbiamo la tesi. □

Nel caso particolare in cui M sia finitamente generato vale la seguente proposizione.

Proposizione 4.3.2. *M finitamente generato $\Rightarrow$ M è isomorfo ad un quoziente di $A^n \cong A \oplus \cdots \oplus A$ (n volte).*

Dimostrazione. Sia $\{m_1, \cdots, m_k\}$ un insieme di generatori per M. Consideriamo la mappa

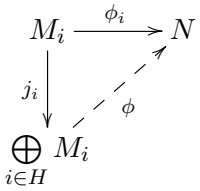
$$\begin{aligned} \phi : A^k &\longrightarrow M \\ e_j &\longmapsto m_j \end{aligned}$$

Gli m_i generano, quindi f è surgettiva e $M \cong A^k \,/\, Ker f$ per il Primo Teorema di Omomorfismo. □

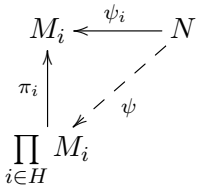
Osservazione. Il viceversa è ovvio, quindi effettivamente si tratta di un *se e solo se*.

Diamo ora come esercizio una importantissima proprietà della somma e del prodotto diretto.

Esercizio (Proprietà Universale della Somma e del Prodotto Diretto)**.** Sia $\{M_i\}_{i \in H}$ una famiglia di A-moduli, N un A-modulo, e $\forall i \in H \ \exists \phi_i : M_i \longrightarrow N$. Se $j_i : M_i \hookrightarrow \bigoplus_{i \in H} M_i$ è l'inclusione canonica, allora $\exists \phi : \bigoplus_{i \in H} M_i \longrightarrow N$ tale che $\phi \circ j_i = \phi_i$, ovvero ϕ fa commutare il seguente diagramma.



In maniera del tutto analoga, se consideriamo il prodotto diretto $\prod_{i\in H} M_i$ e supponiamo che $\forall i \in H\ \exists \psi_i : N \longrightarrow M_i$ allora $\exists \psi : N \longrightarrow \prod_{i\in H} M_i$ che fa commutare il diagramma.



4.4 Da Hamilton-Cayley al Lemma di Nakayama

Teorema 4.3 (Teorema di Hamilton-Cayley)**.** *Sia M un A-modulo finitamente generato, $I \subseteq A$ un ideale, $f : M \to M$ un omomorfismo tale che $f(M) \subseteq IM$. Allora $\exists a_0, \cdots, a_{n-1} \in I$ tali che $f^n + \sum_{j=1}^{n-1} a_j f^j \equiv 0$.*

Dimostrazione. Sia $B = \{m_1, \cdots, m_n\}$ un insieme di generatori. Allora $\forall i = 1, \cdots, n\ f(m_i) = \sum_{j=1}^{n} c_{ij} m_j \Leftrightarrow \sum_j (\delta_{ij} f - c_{ij}) m_j = 0$, dove i $c_{ij} \in I$. Abbiamo dunque un sistema di n equazioni la cui matrice dei coefficenti è la seguente:

$$\begin{bmatrix} f - c_{11} & \cdots & -c_{1n} \\ & & \\ -c_{n1} & \cdots & f - c_{nn} \end{bmatrix}$$

Chiamiamo tale matrice T, e moltiplichiamola per la matrice T^* tale che

$$T^*T = \begin{bmatrix} detT & \cdots \\ & \\ \cdots & detT \end{bmatrix}$$

T^* è la trasposta della matrice dei cofattori, nota anche come matrice aggiunta, ed è la matrice che rappresenta l'algoritmo necessario per ottenere l'inversa sfruttando l'algoritmo di Laplace. Abbiamo dunque $detT \in I[f]$ che si annulla in tutti gli $m_i \Rightarrow$ abbiamo il polinomio che cercavamo. □

Da questo teorema deriva un importantissimo lemma, che presenteremo in tre forme diverse e che ci sarà spesso utile.

Lemma 4.4.1 (Lemma di Nakayama)**.** *Sia $I \subseteq A$ ideale, M un A-modulo finitamente generato.*

1. $M = IM \Rightarrow \exists a \in A \mid a \equiv 1 \ (I) \wedge aM = 0$.
2. *Sia* $I \subseteq \mathfrak{J}(A)$. $M = IM \Rightarrow M = 0$.
3. $I \subseteq \mathfrak{J}(A), N \subseteq M$ *sottomodulo.* $M = IM + N \Rightarrow M = N$.

Dimostrazione. Dedichiamoci alle tre forme una per volta.

1. Sia $f = \mathrm{id}_M$. Chiaramente $f(M) \subseteq M = IM \Rightarrow$, quindi possiamo applicare Hamilton-Cayley e affermare che

$$\exists a_0, ..., a_{n-1} \in I \mid id^n + \sum_{j=0}^{n-1} a_j id^j = id(1 + \sum_{j=0}^{n-1}) \equiv 0$$

   ovvero

$$\exists a \in M \mid a \equiv 1 \ (I) \wedge am = 0 \ \forall m \in M \Leftrightarrow a \equiv 1 \ (I) \wedge aM = 0.$$

2. Per la prima forma del lemma sappiamo che $\exists a \in A \mid aM = 0$; vorremmo mostrare che necessariamente da questo segue che $M = 0$. $a - 1 \in I \Rightarrow 1 + (a - 1) = a \in A^* \Rightarrow aM = 0 \Leftrightarrow a^{-1}aM = M = 0$.
3. Vorremmo applicare la seconda formulazione del lemma a $M \,/\, N \Rightarrow$ vogliamo mostrare che $I(M \,/\, N) = M \,/\, N$. Osserviamo che

$$I({}^{M}\!/_{N}) = \{\sum_i a_i(m_i + N) \mid a_i \in I, m_i \in M\} =$$

$$= \{\sum_i a_i m_i + N \mid a_i \in I, m_i \in M\} = {}^{IM + N}\!/_{N}$$

   ma $IM + N = M \Rightarrow I(M \,/\, N) = M \,/\, N$.

□

Vediamo una prima applicazione di questo lemma.

Esercizio. Sia M un A-modulo finitamente generato, A un anello locale ed $\mathfrak{m}$ il suo ideale massimale. Se $m_1, \cdots, m_k \in M$ sono tali che $\{\pi(m_1), \cdots, \pi(m_k)\}$ generano $M \,/\, \mathfrak{m}M \Rightarrow m_1, \cdots, m_k$ generano M.

Dimostrazione. Sia $N =< m_1, \cdots, m_k > \subseteq M$. Osserviamo che $(\pi \circ j) : N \hookrightarrow M \twoheadrightarrow M \,/\, \mathfrak{m}M$ è surgettiva, da cui $N = M + \mathfrak{m}M \Rightarrow M = N$ poichè $\mathfrak{m} \subseteq \mathfrak{J}(A)$ in quanto A è locale. □

Questo esercizio ci dà un lower bound sulla base di M, poichè $\mathfrak{m}$ massimale $\Leftrightarrow A/\mathfrak{m}$ campo, da cui si deduce che $M/\mathfrak{m}M$ è uno spazio vettoriale su $A/\mathfrak{m} \Rightarrow$ tutte le sue basi hanno medesima cardinalità $\Rightarrow$ per generare M serviranno almeno k elementi. In altre parole, il Lemma di Nakayama ci permette di dimostrare che nel caso di anelli locali con ideale massimale $\mathfrak{m}$, ogni base dello spazio vettoriale $M/\mathfrak{m}M$ si solleva a insieme minimale di generatori di M, da cui, appunto, il *lower bound* di cui parlavamo.
Questo è sicuramente un gran passo in avanti, ma molte questioni rimangono irrisolte perchè il concetto di dimensione, e i risultati che ne derivano, continua a rimanere un lontano ricordo. Non perdiamo però la speranza e dimostriamo il seguente risultato.

Proposizione 4.4.1. *Sia $f : M \longrightarrow M$ omomorfismo di A-moduli. Se M è finitamente generato allora vale che f surgettivo $\Rightarrow f$ iniettivo.*

Dimostrazione. M è un A-modulo finitamente generato, ma in questo caso ci sarà più utile vederlo come $A[x]$-modulo. Chiaramente dobbiamo definire il prodotto: se $p(x) \in A[x], m \in M$ allora

$$p(x) \cdot m = (\sum_{i=0}^{n} a_i x^i) \cdot m = \sum_{i=0}^{n} a_i f^i(m) \in M.$$

Facciamo questa scelta perchè $f(m) = x \cdot m \ \forall m \in M$ e $Imf = M = \{f(m) \mid m \in M\}$ per surgettività di f. Infatti possiamo ora affermare che $Imf = \{x \cdot m \mid m \in M\} = (x)M \Leftrightarrow (x)M = M$, e applicare la prima formulazione del Lemma di Nakayama e affermare che $\exists p(x) \in A[x]$ tale che $p(x)M = 0 \wedge p(x) \equiv 1\ (x)$, ovvero $p(x) = 1 + xq(x)$. Sfrutteremo questa informazione per dimostrare che f è iniettiva. $p(x) \in Ann(M)$, quindi, in particolare, possiamo scegliere $m \in Kerf$ e vale che $p(x) \cdot m = 0 = (1 + xq(x)) \cdot m = m + q(x) \cdot f(m) = m \Rightarrow Kerf = \{0\} \Leftrightarrow f$ è iniettiva. □

Corollario 4.3.1. *Se M è libero di rango $n \Rightarrow$ ogni insieme di generatori con n elementi è una base.*

Dimostrazione. M libero di rango n, quindi, in particolare, è finitamente generato $\Leftrightarrow$ è isomorfo ad un un quoziente di A^n; ma M è libero $\Rightarrow$ è isomorfo ad A^n. Fissiamo allora un insieme di generatori $< m_1, \cdots, m_n >$ e osserviamo che $M \overset{f}{\cong} A^n \overset{g}{\twoheadrightarrow} M$, dove $f(m_i) = e_i$ e $g(e_i) = m_1$. Per come abbiamo scelto gli m_i abbiamo che $g \circ f$ è surgettiva, quindi abbiamo un *endomorfismo* surgettivo di un modulo M finitamente generato $\Rightarrow$ è anche iniettivo $\Rightarrow g \circ f$ è un isomorfismo. Di conseguenza $(g \circ f) \circ f^{-1} = g$ è ancora un isomorfismo, in quanto composizione di isomorfismi. □

Diamo subito degli esempio di applicazione di questo risultato.

Esercizio (Esame parziale del 20 Aprile 2011)**.** Sia M un A-modulo finitamente generato e sia $(0) \neq N \subseteq M$ un sottomodulo. Dimostrare che $M \ncong M \,/\, N$ e dare un controesempio per il caso in cui M non è finitamente generato.

Dimostrazione. Supponiamo di disporre di un isomorfismo $f : M \,/\, N \longrightarrow M$. Allora $f \circ \pi : M \overset{\pi}{\twoheadrightarrow} M \,/\, N \xrightarrow{f} M$ è una mappa surgettiva da M in M; poichè però M è finitamente generato possiamo dedurre che sia iniettiva $\Rightarrow f^{-1} \circ (f \circ \pi) = \pi$ è isomorfismo in quanto composizione di isomorfismo $\Leftrightarrow N = (0)$, assurdo per ipotesi.
Il controesempio ci è dato da $\mathbb{K}[x_1, \cdots, x_n \cdots]$ anello dei polinomi in infinite variabili a coefficenti in $\mathbb{K}$: scegliamo $N = (x_1)$ e osserviamo che in questo caso $\pi : M \longrightarrow M \,/\, N$ è un isomorfismo di moduli. □

Esercizio. Sia $I \subseteq \mathfrak{J}(A)$, A anello, e M un A-modulo. Sia $N \subseteq M$ finitamente generato e $\phi M \longrightarrow N$. Se $\overline{\phi} : M \,/\, IM \longrightarrow N \,/\, IN$ è surgettiva $\Rightarrow \phi$ è surgettiva.

Dimostrazione. Il radicale di Jacobson e la proprietà di essere finitamente generato devono farci immediatamente venire in mente Nakayama. Vediamo dunque come applicarlo.
Abbiamo, fondamentalmente, il seguente diagramma:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ {\scriptstyle \pi_M}\downarrow & & \downarrow{\scriptstyle \pi_N} \\ M \,/\, IM & \xrightarrow{\overline{\phi}} & N \,/\, IN \end{array}$$

Osserviamo che $\forall n{+}IN\ \exists m{+}IM \mid \overline{\phi}(m{+}IM) = (n{+}IN) \Leftrightarrow \phi(m){+}\phi(IM) = n{+}IN$, da cui $N = Im\phi{+}IN$. Applichiamo la terza formulazione del Lemma di Nakayama e otteniamo $N = Im\phi$. □

4.5 Successioni Esatte

Definizione 4.5.1. *Sia $\{M_i\}_{i \in H}$ una famiglia di A-moduli, e $\{f_i\}_{i \in H}$ una famiglia di omomorfismi tale che:*

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

Una successione di questo tipo è detta esatta *se $\forall i \in i$ vale $Ker f_{i+1} = Im f_i$.*

Alcuni casi notevoli di successioni esatte sono i seguenti.

i) $0 \longrightarrow M \xrightarrow{f} N \Leftrightarrow f$ è iniettiva;

ii) $M \xrightarrow{g} P \longrightarrow 0 \Leftrightarrow g$ è surgettiva;

iii) $0 \longrightarrow M \overset{f}{\hookrightarrow} N \overset{g}{\twoheadrightarrow} P \longrightarrow 0$ è esatta corta se è esatta.

D'ora in avanti sentiremo spesso parlare di successioni che *spezzano*, ovvero di successioni che ci permettono di dedurre delle informazioni molto forti sulla struttura dei moduli che coinvolgono. In simboli, ci troveremo di fronte a successioni del tipo:

$$0 \longrightarrow M \overset{i}{\hookrightarrow} M \oplus N \overset{\pi}{\twoheadrightarrow} N \longrightarrow 0$$

dove il modulo "di mezzo" è esprimibile, chiaramente, come somma diretta degli altri due.
Ci chiediamo, dunque, sotto quali ipotesi una successione esatta corta *spezzi*. A darci risposta è la seguente proposizione.

Proposizione 4.5.1. *Siano M, N, P A-moduli e siano α, β omomorfismi tali che la seguente sia una successione esatta corta:*

$$0 \longrightarrow M \overset{\alpha}{\hookrightarrow} N \overset{\beta}{\twoheadrightarrow} P \longrightarrow 0$$

Allora le seguenti sono equivalenti:

1. $N \cong M \oplus P \Leftrightarrow$ *la successione spezza;*
2. $\exists r : M \longrightarrow N \mid \alpha \circ r = \mathrm{id}_M$, *detta* ***retrazione****;*
3. $\exists s : P \longrightarrow N \mid \beta \circ s = \mathrm{id}_P$, *detta* ***sezione****.*

Dimostrazione. Facciamo vedere le varie implicazioni.

1) $\Rightarrow$ 2), 3) Ovvio.

2) $\Rightarrow$ 1) Per ipotesi $\exists r : M \longrightarrow N \mid r \circ \alpha = \mathrm{id}_M$. Vogliamo far vedere che $N = M \oplus P$. Cominciamo osservando che $\forall n \in N$, $n = (n - \alpha(r(n))) + \alpha(r(n))$. Sia allora $L =< n - \alpha(r(n)) \mid n \in N >$. Chiaramente $N \cong L + Im\alpha$; ora vorremmo mostrare che la somma è diretta, e dunque che $L \cap Im\alpha = \{0\}$. Sia dunque $\alpha(m) = n - \alpha(r(n))$ un elemento dell'intersezione. Applicando r si ottiene $r(\alpha(m)) = r(n) - r(\alpha(r(n)) = 0$ per definizione di $r \Rightarrow N \cong Im\alpha \oplus L$[2].
Ci resta da vedere che $M \cong Im\alpha$ e $P \cong L$. Cominciamo dimostrando che $\beta|_L$ è isomorfismo, da cui $P \cong L$.

Iniettività: $\beta|_L(n - \alpha(r(n)) = 0 \Leftrightarrow \beta(n) = \beta(\alpha(r(n))) = 0$ perchè $\beta \circ \alpha = 0$ per esattezza. , dunque $n = 0$;

[2]Potreste, a questo punto, essere tentati di concludere quozientando. Tuttavia, nonostante via sia la somma diretta, non è sempre vero che $N \cong L \oplus P \Rightarrow P \cong N / L$ per via dell'isomorfismo. Se invece vale l'uguaglianza allora è vero.

Surgettività: $\forall p \in P\ \exists n \in N$ tale che $\beta(n) = p$ perchè $P \cong N\,/\,Im\alpha$ per esattezza della successione.

Sia dunque $\phi : N \longrightarrow Im\alpha \oplus L \mid n \longmapsto \phi(n) = \phi(\alpha(r(n)), n - \alpha(r(n))) = (r(n), \beta(n - \alpha(r(n))))$. Poichè $(\phi \circ \alpha)(m) = \phi(\alpha(m), 0) = (m, 0)$ è un'immersione e $(\beta \circ \phi^{-1})(m, P) = \beta(\alpha(m), (\beta|_L)^{-1}P) = (0, P) = P$, ϕ è l'isomorfismo che cercavamo.

Con la medesima idea si dimostra che 3) $\Rightarrow$ 1). □

4.5.1 Il Funtore Hom

In questa sezione vogliamo studiare il modo in cui vengono trasformate successioni esatte tra moduli. Per capire in che senso venga applicata una trasformazione ci servirà il linguaggio della Teoria delle Categorie.

Definizione 4.5.2. *Una categoria $\mathscr{C}$ consiste di una classe di oggetti $Obj(\mathscr{C})$ e una classe di frecce $Hom(\mathscr{C})$ tra questi oggetti, dette anche morfismi o mappe. Si richiede che sia ben definita la composizione tra morfismi, che sia associativa, e che per ogni oggetto in $\mathscr{C}$ esista il morfismo identico.*

Degli esempi sono la categoria degli insiemi, Set, i cui morfismi sono le applicazioni tra insiemi, oppure la categoria degli anelli, Ring, i cui morfismi sono gli omomorfismi di anelli. Un'altra categoria con cui abbiamo già avuto a che fare è Top, i cui oggetti sono gli spazi topologici e le cui mappe sono le funzioni continue.

Vorremo adesso definire delle mappe tra categorie. Non avendo mai avuto a che fare con oggetti di questo tipo, dobbiamo dare una nuova definizione.

Definizione 4.5.3. *Sia $\mathscr{C}$ e (D) due categorie. Definiamo funtore una mappa $F : \mathscr{C} \longrightarrow \mathcal{D}$ tale che ad ogni oggetto in $\mathscr{C}$ sia associato un oggetto in (D),e che ad ogni mappa in $Hom(\mathscr{C})$ sia associata una mappa in $Hom(\mathcal{D})$. In particolare, richiediamo che per ogni oggetto A in $\mathscr{C}$ valga*

$$F(\mathrm{id}_A) = \mathrm{id}_{F(A)}\,.$$

Un funtore può agire in due modi diversi:

- si dice **funtore covariante** se $F(f) : F(A) \longrightarrow F(B)$;
- si dice **funtore controvariante** se $F(f) : F(B) \longrightarrow F(A)$.

Se dunque consideriamo la composizione di due morfismi si ha:

- $F(g \circ f) = F(g) \circ F(f)$ se F è covariante;
- $F(g \circ f) = F(f) \circ F(g)$ se F è controvariante.

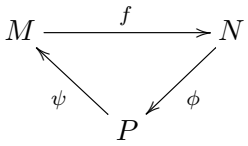
Un esempio di funtore è dato dal funtore costante che mappa un'intera categoria in un oggetto di un'altra, e ogni morfismo nell'identità su tale oggetto. Alternativamente, possiamo considerare un funtore del tipo seguente:

$$F : \text{Ring} \longrightarrow \text{Set}$$
$$R \longrightarrow R$$

In questi casi si parla di *funtore dimenticante*, poichè essenzialmente causa la perdita di varie informazioni sulla struttura degli oggetti della categoria.

Ora che possiamo pronunciare con coscienza la parola "funtore", passiamo al caso particolare che è di nostro interesse.

Siano M, N, P tre A-moduli, e siano f, ϕ, ψ omomorfismi di moduli definiti come nel seguente diagramma.



Definiamo le mappe:

$$f^* : Hom_A(N, P) \longrightarrow Hom_A(M, P) \mid \phi \longmapsto f^*(\phi) = \phi \circ f$$

$$f_* : Hom_A(P, M) \longrightarrow Hom_A(P, N) \mid \psi \longmapsto f_*(\psi) = f \circ \psi$$

Queste mappe ci permettono di associare a successioni esatte di moduli delle successioni in cui i moduli che compaiono sono della forma $Hom_A(M, N)$. In questo senso, si comportano come dei funtori, e in quanto tali possono essere studiati. Precisamente, queste mappe altro non sono che due tipi di funtore Hom:

- $f^* = Hom(\_, P)$ tale che $Hom(\_, P)(Hom_A(N, P)) \subseteq Hom(M, P)$
- $f_* = Hom(P, \_)$ tale che $Hom(P, \_)(Hom_A(P, M)) \subseteq Hom_A(P, N)$

Attraverso questi due funtori vedremo in che senso possiamo trasformare delle successioni esatte.

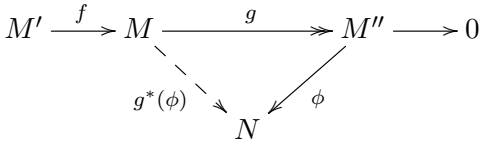
Proposizione 4.5.2. *Siano M, M', M'' A-moduli. Allora:*

1. $M' \xrightarrow{f} M \overset{g}{\twoheadrightarrow} M'' \longrightarrow 0$ *è esatta* $\Leftrightarrow \forall N$ *A-modulo* $0 \longrightarrow Hom(M'', N) \xrightarrow{g^*} Hom(M, N) \xrightarrow{f^*} Hom(M', N)$ *è esatta;*

2. $0 \longrightarrow M' \overset{f}{\hookrightarrow} M \xrightarrow{g} M''$ *è esatta* $\Leftrightarrow \forall N$ *A-modulo* $0 \longrightarrow Hom(N, M') \xrightarrow{f_*} Hom(N, M) \xrightarrow{g_*} Hom(N, M')$ *è esatta.*

Dimostrazione. Iniziamo con la dimostrazione del primo punto.

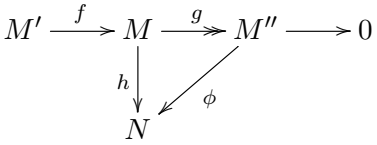
(⇒) Supponiamo che $M' \xrightarrow{f} M \overset{g}{\twoheadrightarrow} M'' \longrightarrow 0$ sia esatta. Dobbiamo dimostrare che g^* è iniettiva e che $Kerf^* = Img^*$. Siamo dunque in questa situazione:



Dimostrare l'iniettività di g^* equivale a mostrare che $g^*(\phi) = 0 \Leftrightarrow \phi = 0$. Sfruttiamo il diagramma: $g^*(\phi) = 0 \Leftrightarrow (\phi \circ g)(m) = 0 \forall m \in M$. g è surgettiva $\Rightarrow \forall m'' \in M''$, $m'' = g(m)$ per qualche $m \in M$, dunque $(\phi \circ g)(m) = 0 \forall m \in M \Rightarrow \phi(m'') = 0 \forall m'' \in M''$, dunque ϕ è identicamente nulla.
Ora vogliamo mostrare che $Kerf^* = Img^*$; vediamo le due inclusioni.

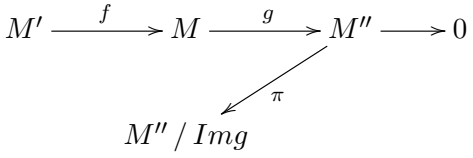
(⊇) Sia $h \in Img^* \Leftrightarrow h = g^*(\phi) \Leftrightarrow h = \phi \circ g$. Allora si ha $f^*(h) = h \circ f = (\phi \circ g) \circ f = \phi \circ (g \circ f) = \phi \circ 0 = 0$, dove $g \circ f = 0$ per ipotesi di esattezza sulla successione.

(⊆) Sia ora $h \in Kerf^*$. Per far chiarezza sul nostro obiettivo, consideriamo il seguente diagramma.



Vogliamo far vedere che $\forall N$ A-modulo $\exists \phi \in Hom(M'', N)$ tale che $g^*(\phi) = h$, quindi dovremo definire un omomorfismo che soddisfi le nostre richieste. Vediamo come.
Per ipotesi, sappiamo che g è surgettiva, ovvero $\forall m'' \in M'' \; \exists m \in M$ tale che $g(m) = m''$; allora, poichè vorremmo che il diagramma commutasse, proviamo a definire $\phi(m'') = h(m)$. É una buona definizione? Lo è se h rispetta le fibre di g; verifichiamolo.
Sia $\tilde{m} \in M$ tale che $g(m) = g(\tilde{m}) = m'' \Leftrightarrow g(m - \tilde{m}) = 0 \Leftrightarrow m - \tilde{m} \in Imf$; ma $h \circ f = 0 \Rightarrow h(m - \tilde{m}) = 0 \Leftrightarrow h(m) = h(\tilde{m})$, quindi la definizione è ben posta e l'inclusione è dimostrata.

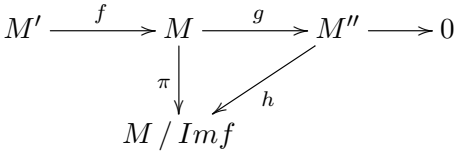
(⇐) Per mostrare l'esattezza della successione scegliamo $N = M'' / Img$. Dunque abbiamo



La successione è esatta se g è surgettiva, quindi vogliamo mostrare che $M'' \,/\, Img = 0$, ovvero che π è identicamente nulla. Osserviamo che $g^*(\pi)(m) = (\pi \circ g)(m) = 0 \Rightarrow g^*(\pi) = 0$; ma la successione sui moduli di omomorfismi è esatta, quindi in particolare g^* è iniettiva $\Rightarrow \pi = 0 \Rightarrow Img = M'' \Leftrightarrow g$ è surgettiva.
Ora dobbiamo mostrare che $Kerg = Imf$; affrontiamo le due inclusioni separatamente.

($\supseteq$) Sia $m = f(m') \Rightarrow g(m) = g(f(m')) = (f^*(g))(m)$; vorremmo verificare che $f^*(g)(m) = 0$, ovvero che $g \in Kerf^*$. Per ipotesi di esattezza sulla successione, sappiamo che $\forall N$ modulo vale che $Kerf^* = Img^*$; scegliamo dunque $N = M''$. Allora $g \in Kerf^* = Img^* \Leftrightarrow \exists h \in Hom(M'', M'') \mid h \circ g = g$. Poichè l'identità è un omomorfismo di moduli possiamo scegliere $h = \mathrm{id}_{M''} \Rightarrow g = g^*(\mathrm{id}_{M''}) \Rightarrow g \in Img^* = Kerf^*$. Allora $f^*(g)(m') = 0 \ \forall m' \in M' \Leftrightarrow (g \circ f)(m') = 0 \Leftrightarrow Imf \subseteq Kerg$.

($\subseteq$) Scegliamo ora $N = M \,/\, Imf$.



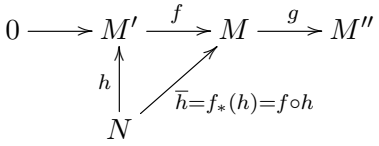
Osserviamo che $f^*(\pi) = (\pi \circ f) = 0 \Rightarrow \pi \in Kerf^* = Img^*$ per esattezza della successione. Allora $\exists h \in Hom(M'', M \,/\, Imf \mid g^*(h) = h \circ g = \pi$ perchè $\pi \in Kerf^* = Img^* \Rightarrow Ker\pi \supseteq Kerg$; ma $Ker\pi = Imf \Rightarrow Kerg \subseteq Ker\pi = Imf$.

Proseguiamo ora con il secondo punto.

($\Rightarrow$) Assumiamo che $0 \longrightarrow M' \overset{f}{\hookrightarrow} M \overset{g}{\longrightarrow} M''$ sia esatta $\Leftrightarrow Kerf = \{0\} \wedge Imf = Kerg$, e mostriamo che $Kerf_* = \{0\}$ e che $Imf_* = Kerg_*$.
Iniziamo con l'iniettività di f_*: sia $h \in Kerf_* \Leftrightarrow f_*(h) = f \circ h = 0 \Leftrightarrow Imh \subseteq Kerf$; ma f è iniettiva $\Rightarrow Imh \in \{0\} \Leftrightarrow h = 0$.
Ora mostriamo che $Imf_* = Kerg_*$.

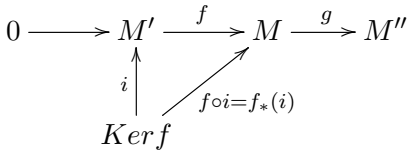
($\subseteq$) Sia $\overline{h} \in Imf_* \Leftrightarrow \exists h \in Hom(N, M') : \overline{h} = f \circ h$. Dunque $g_*(\overline{h}) = g \circ \overline{h} = (g \circ f) \circ h = 0 \circ h = 0$ per esattezza.

($\supseteq$) Vogliamo mostrare che se $g_*(\overline{h}) = 0 \Rightarrow \exists h \in Hom(N, M') : f_*(h) = \overline{h}$, quindi proviamo a costruire h tale che $f \circ h = \overline{h}$. Per chiarire la situazione osserviamo il diagramma.



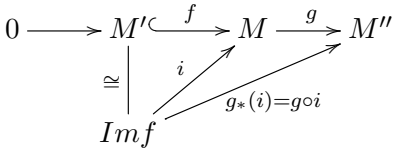
Sappiamo che f è iniettiva $\Leftrightarrow \forall m \in M \exists! m' \in M' \mid f(m') = m$. Ora concentriamoci su $\overline{h}$ e osserviamo che $g_*(\overline{h}) = g \circ \overline{h} = 0 \Rightarrow Im\overline{h} \subseteq Kerg = Imf$. Dunque $\forall m \in Im\overline{h}\ \exists! m' \in M', \exists n \in N \mid \overline{n} = m \wedge f(m') = m$; sia allora $h(n) = m$.
Si tratta di una buona definizione? Sì perchè f è iniettiva e stiamo associando ad un elemento $n \in N$ l'unico elemento $m' \in M'$ tale che $f(m') = \overline{h}(n)$. Con questa definizione si ha che $f_*(h) = f \circ h = \overline{h}$, da cui $Kerg_* \subseteq Imf_*$.

($\Leftarrow$) Supponiamo ora che $\forall N\ 0 \longrightarrow Hom(N, M') \xrightarrow{f_*} Hom(N, M) \xrightarrow{g_*} Hom(N, M'')$ sia esatta $\Leftrightarrow Imf_* = Kerg_* \wedge Kerf_* = \{0\}$. Vogliamo mostrare che $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ è esatta $\Leftrightarrow Kerf = \{0\} \wedge Imf = Kerg$. Come prima, cominciamo con l'iniettività di f; per farlo scegliamo $N = Kerf$. Abbiamo dunque



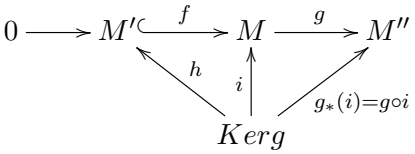
Chiaramente $f_*(i) = 0$, ma f_* è iniettiva $\Rightarrow i = 0 \Leftrightarrow Kerf = \{0\} \Leftrightarrow f$ è iniettiva.
Dimostriamo ora che $Kerg = Imf$.

($\supseteq$) Scegliamo $N = Imf$; f è iniettiva $\Rightarrow Imf \cong M'$. Siamo dunque nella seguente situazione:



$i \in Imf_* \Leftrightarrow \exists h \in Hom(Imf, M') \mid f \circ h = f_*(h) = i$ perchè f è iniettiva ed è quindi un isomorfismo su Imf; ma $Imf_* = Kerg_* \Rightarrow g_*(i) = g \circ i = 0 \Leftrightarrow Imf \subseteq Kerg$.

($\subseteq$) Sia $m \in Kerg$; vogliamo dimostrare che $\exists m' \in M' \mid f(m') = m$. Sia ora $N = Kerg$. $i \in Kerg_* = Imf_* \Leftrightarrow \exists h \in Hom(Kerg, M')$ tale che $f \circ h = f_*(h) = i$. Dunque abbiamo



dove $f_*(i) = f \circ h = i$. i ed f sono iniettive, quindi h deve essere iniettiva $\Rightarrow Kerg \subseteq Imf$.

□

Chi ha seguito le lezioni saprà che la dimostrazione del secondo punto non è stata svolta a lezione, e quindi deduce facilmente che è stata pensata e scritta da me. Di conseguenza, se notate errori o avete osservazioni da fare, sarò più che contenta di prenderne atto.

Ora che disponiamo delle successioni esatte, diamo sotto forma di esercizio un risultato sulle somme dirette di moduli che ci sarà utile nel prossimo teorema.

Esercizio. Se $M_1, M_2 \subseteq M$ sono sottomoduli, allora vale sempre che $0 \longrightarrow M_1 \cap M_2 \overset{f}{\hookrightarrow} M_1 \oplus M_2 \overset{g}{\twoheadrightarrow} M_1 + M_2 \longrightarrow 0$, dove $f(m) = (m, m)$ e $g(m_1, m_2) = m_1 + m_2$), è sempre una successione esatta.

4.6 Moduli su PID

Sia M un modulo libero di rango finito su un qualsiasi anello A. Se il rango è r, allora si mostra facilmente che

$$M \cong \bigoplus_{j=1}^{r} A = A^r$$

Per convincercene, è sufficiente fissare una base $< m_1, \cdots, m_r >$ e osservare che ogni elemento di M si scrive in modo unico come combinazione a coefficenti in A di elementi della base, dunque $\exists f : A^r \twoheadrightarrow M \mid e_i \mapsto m_i$. Poichè, infine, $(a_1, \cdots, a_r) \in Kerf \Leftrightarrow \sum_{i=1}^{r} a_i m_i = 0$, si conclude che $Kerf = \{0\}$ per lineare indipendenza degli elementi della base.
Per quelli che però sono i nostri scopi, il fatto che M sia libero non è sufficiente. Ad esempio, se $N \subseteq M$ è un sottomodulo, non è detto che sia libero – un esempio ci è dato da $(x, y) \subseteq \mathbb{K}[x, y]$ visti come moduli su $\mathbb{K}[x, y]$: $\mathbb{K}[x, y]$ è generato da $\{1\}$, ma (x, y) non ammette base, giacché $xy - yx = 0$. Ci servono dunque delle ipotesi più forti: sia A PID.

Teorema 4.4. *Se M è modulo libero su A PID, e $(0) \neq N \subseteq M$ è un sottomodulo $\Rightarrow$ N è libero e $rkN \leq rkM$.*

Dimostrazione. Per semplicità, affrontiamo solo il caso di rango finito. Quello di rango infinito segue sostanzialmente dalla medesima idea, ma è tecnicamente più complicato.
Procediamo per induzione su r.

P:B.: $r = 1$, allora $M =< m >$ è un modulo ciclico. $f : A \longrightarrow M \mid 1 \mapsto m$ è chiaramente un isomorfismo di moduli $\Leftrightarrow$ M è libero. Allora N è isomorfo ad un sottomodulo di A visto come modulo su sè stesso, ovvero N è isomorfo ad un ideale di A. A è PID $\Rightarrow N \cong (a)$. Poichè, infine,

$ka = 0 \Rightarrow k = 0$ per integrità di A, abbiamo che N è libero perchè lo è (a).

P.I.: Assumiamo l'ipotesi vera per r e consideriamo M di rango $r+1$ con base $< m_1, \cdots, m_{r+1} >$. Sia $(0) \neq N \subseteq M$ e sia $N_r = N \cap < m_1, \cdots, m_r >$. $N_r \subseteq < m_1, \cdots, m_r >$ modulo libero di rango $r \Rightarrow N_r$ è libero di rango $\leq r$. Arrivati a questo punto, possono verificarsi due cose:

1. $N = N_r$, e in questo caso abbiamo concluso;
2. $N \supsetneq N_r$, da cui deduciamo che $\exists n \in N \mid n = b_1 m_1 + \cdots + b_r m_r + a_n m_{r+1}$

Per affrontare questo secondo caso ci servirà qualche ulteriore osservazione. Cominciamo introducendo

$$I := \{\alpha \in A \mid \exists n \in N : n = b_1 m_1 + \cdots + b_r m_r + \alpha m_{r+1}\},$$

dove $b_1, ..., b_r$ variano a seconda di n.
Si verifica facilmente che I è non vuoto in quanto $0 \in I$, e che I è un ideale. Poichè A è PID, $I = (d), d \neq 0 \Rightarrow \exists n_d \in N \mid n_d = c_1 m_1 + \cdots + c_r m_r + d m_{r+1}$.

CLAIM: $N \cong N_1 \oplus < n_d >$.

Sia $n \in N$, $n = b_1 m_1 + \cdots + b_r m_r + a_n m_{r+1} \Rightarrow \exists k \in A \mid a_n = kd$, quindi possiamo scrivere $n = (n - k n_d) + k n_d \Rightarrow N = N_2 + < n_d >$. Per concludere che la somma interna coincida con la somma diretta dobbiamo far vedere che $n \in N_2 \cap < n_d > \Rightarrow n = 0$; ma se un tale n è della forma $n = b_1 m_1 + \cdots + b_r m_r = k d m_{r+1} \Rightarrow (b - k c_1) m_1 + \cdots + (b_r + k c_r) - k d m_{r+1} = 0 \Rightarrow kd = 0 \Rightarrow k = 0 \Rightarrow b_i = 0 \ \forall i = 1, \cdots, r$, quindi l'interesezione è il solo 0.
La somma diretta di moduli liberi è libera, da cui la tesi.

□

Osservazione. Se M è modulo su A PID ed è finitamente generato, possiamo concludere che un suo qualsiasi sottomodulo N è anch'esso finitamente generato e di rango minore o uguale. Se infatti $f : A^r \twoheadrightarrow M \cong M / Ker f \Rightarrow f^{-1}(N) \subseteq A^r$ è libero e di rango $\leq r \Rightarrow$ è finitamente generato.

Queste proprietà sono tutto quello che ci serve per dimostrare un importante teorema di struttura per moduli finitamente generati su anelli a ideali principali.

Teorema 4.5. *Sia M modulo finitamente generato su A PID. Allora vale la seguente affermazione:*

$$M \cong A^k \oplus T(M), \qquad T(M) := \{m \in M \mid \exists a \in A, a \neq 0, \ am = 0\}$$

Dimostrazione. M è finitamente generato $\Rightarrow 0 \longrightarrow Kerf \hookrightarrow A^r \overset{f}{\twoheadrightarrow} M \longrightarrow 0, Kerf \subseteq A^r$ sottomodulo anch'esso libero.
Più precisamente, se scegliamo la base canonica $\{e_j\}_{j=1,\cdots,r}$ per A^r e fissiamo $< m_1, \cdots, m_r >$ insieme di generatori di M, $f(e_j) = m_j$ e $Kerf =< w_1, \cdots, w_s >$, da cui un'altra successione esatta:

$$0 \longrightarrow A^s \overset{g}{\hookrightarrow} A^r \overset{f}{\twoheadrightarrow} M \longrightarrow 0, \quad g(e_j) = w_j,\ f(e_j) = m_j$$

Applicando i teoremi di omomorfimo abbiamo

$$M \cong A^r /_{Kerf} \cong A^r /_{Img} = cokerg.$$

Il nostro obiettivo sarà adesso quello di esprimere g in forma ottimale per poterne esprimere il *coker*, e quindi per poter dare una struttura ad M. Ci vengono in aiuto le idee già viste nei corsi di Algebra Lineare: g è una mappa A lineare da A^s in $A^r \Rightarrow$ può essere vista come matrice $r \times s$.

Osservazione. Sarà utile ricordare che una matrice a coefficenti in un PID è invertibile $\Leftrightarrow$ il suo determinante è un'unità del dominio.

In che modo, dunque, possiamo manipolare la matrice che rappresenta g? Dobbiamo rispettare la struttura di A, quindi possiamo effettuare operazioni elementari del tipo:

- scambio di due righe;
- sommare ad una riga il multiplo di un'altra riga;
- moltiplicare per degli invertibili.

Per nostra fortuna, nel caso in cui A è PID vale un risultato analogo (che dimostreremo tra poco) a quello visto per matrici a coefficenti in un campo, ovvero che ogni matrice X di dimensione $r \times s$ è equivalente ad una matrice diagonale $D \Leftrightarrow \exists S, T$ di opportuna taglia tali che $SXT = D$. In particolare, se $d_1, \cdots, d_k$ sono gli elementi sulla diagonale di D, si ha che $d_1 | d_2 | \cdots | d_k$.
Una matrice presentata in una tale forma, si dice essere in Forma di Smith, e quello che dimostreremo adesso è che tale forma è normale. Infatti, se definiamo $\Delta_i = (GCD(\text{determinanti delle sottomatrici } i \times i \text{ di} X)) = (\delta_i)$, si osserva facilmente che $\Delta_i = (\delta_i), \Delta_{i-1} = (\delta_{i-1} d_i) \Rightarrow d_i = \frac{\delta_i}{\delta_{i-1}}$ fintantoché $\delta_{i-1} \neq 0$.
Se dunque $X \sim D \Rightarrow \Delta_i(X) = \Delta_i(D),\ \Delta_1(D) = GDC(d_1, \cdots, d_k) = (d_1), \Delta_2(D) = GDC(d_1 d_2, d_1 d_3, \cdots, d_{n-1} d_n) = (d_1 d_2) = (\delta_2)...$
Ora che disponiamo di una tale presentazione del *cokerg* abbiamo la scrittura di M che desideravamo. □

Chiaramente il nostro prossimo obiettivo è di dimostrare l'unicità di una tale scrittura. Per farlo ci serviranno i seguenti lemmi.

Lemma 4.6.1. *Sia N modulo su A tale che $N \cong A/J_1 \oplus A/J_2$, con J_1, J_2 ideali. Sia $I \subseteq A$ un altro ideale. Allora $N/IN \cong A/J_1 + I \oplus A/J_2 + I$.*

Dimostrazione. $IN \cong I + J_1/J_1 \oplus I + J_2/J_2 \Rightarrow N/IN \cong (A/J_1)/(I + J_1/J_1) \oplus (A/J_2)/(I + J_2/J_2)$, che per il Secondo Teorema di Omomorfismo è isomorfo a $N/IN \cong A/I + J_1 \oplus A/I + J_2$. □

Lemma 4.6.2. *Sia $N = A/J$ un A-modulo, $J \subseteq A$ un ideale, e $a \in A$. Allora $aN \cong A/J : (a))$.*

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} A/J &\longrightarrow aN \\ (b + J) &\longmapsto (ab + J) \end{aligned}$$

Allora abbiamo $A/J \twoheadrightarrow aA/J$ con nucleo evidentemente uguale a $J/(J : (a))$. Dal Primo Teorema di Omomorfismo segue la tesi. □

Lemma 4.6.3. *Sia B un anello e siano $m, n \in \mathbb{N}$ tali che $m > n$. Se esiste un omomorfismo tale che $B^n \twoheadrightarrow B^m \Rightarrow B = \{0\}$.*

Dimostrazione. Vediamo B^n e B^m come B-moduli, ed è dunque chiaro che siano dei moduli finitamente generati.
Osserviamo che possiamo scrivere $B^m = B^n \oplus B^{m-n} \twoheadrightarrow B^n \twoheadrightarrow B^m$. Poichè però stiamo lavorando con moduli finitamente generati sappiamo dal Lemma di Nakayama che un endomorfismo surgettivo è anche iniettivo $\Rightarrow B^{m-n} = \{0\} \Leftrightarrow B = \{0\}$. □

A questo punto dovrei aggiungere la dimostrazione dell'unicità della decomposizone di M, ma lo farò in un secondo momento.

Definizione 4.6.1. *Sia M un A-modulo. Definiamo **d-componente** di M un insieme del tipo $M_d = \{m \in M \mid \exists k \in \mathbb{N} : d^k m = 0\}$. Se p è primo e $M = M_p \Rightarrow M$ si dice p-primario.*

Con questa nuova definizione, possiamo dare un'altra interessante forma alla decomposizione di M appena vista, infatti valgono le seguenti affermazioni:

1. Se M è un A-modulo finitamente generato p-primario, con A PID, allora $M \cong A/(p^{k_1}) \oplus A/(p^{k_2}) \oplus \cdots \oplus A/(p^{k_s})$, con $k_1 < k_2 < \cdots < k_s$.

2. Se M è finitamente generato, allora $M \cong A^k \oplus (\bigoplus_{j=1}^{h} A/(q_j))$ con i (q_j) primari in A, $h, k \geq 0$.

Per passare da una scrittura all'altra, visto che A è PID, basta lavorare con i vari sottomoduli p-primari e poi applicare il teorema cinese del resto per arrivare ai (q_j) primari in A e tali che $q_i | q_j \ \forall i \leq j$.
Per dare maggiori informazioni su $T(M)$, ovvero la cosiddetta *parte di torsione*, è necessario assumere qualche ipotesi in più.

Proposizione 4.6.1. *Sia A dominio, M un A-modulo e $T(M) = \{m \in M \mid \exists a \in A - \{0\} : am = 0\}$. Allora:*

a) $T(M) \subseteq M$ è un sottomodulo;

b) $M \,/\, T(M)$ è libero da torsione;

c) Se $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ è esatta, allora è possibile definire delle mappe tali che $0 \longrightarrow T(M) \longrightarrow T(N) \longrightarrow T(P)$ sia esatta.

Dimostrazione. Dimostriamo i tre punti separatamente.

a) Innanzitutto, osserviamo che $0 \in T(M) \Rightarrow T(M) \neq \emptyset$. Siano ora $m_1, m_2 \in T(M) \Leftrightarrow \exists a_1, a_2 \in A - \{0\} \mid a_1 m_1 = a_2 m_2 = 0 \Rightarrow a_1 a_2 (m_1 + m_2) = 0$ per commutatività dell'anello e per integrità, poichè $a_1 a_2 \neq 0$.

b) $M \,/\, T(M) \ni (m + T(M))$. Se dunque esistesse $a \in A - \{0\}$ tale che $a(m + T(M)) = T(M) \Leftrightarrow am + T(M) = T(M) \Leftrightarrow am \in T(M) \Leftrightarrow m \in T(M)$, dunque $M \,/\, T(M)$ non possiede parte di torsione.

c) Supponiamo che $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ sia esatta e consideriamo $0 \longrightarrow T(M) \xrightarrow{\overline{f}} T(N) \xrightarrow{\overline{g}} T(P) \longrightarrow 0$, dove $\overline{f}, \overline{g}$ sono le mappe date dalle restrizioni di f e g alle parti di torsione. Osserviamo innanzitutto che queste mappe mandano le parti di torsione in parti di torsione: $m \in T(M), \overline{f}(m) = f(m)$, e poichè $\exists a \in A$ tale che $am = 0$ si ha $0 = f(0) = f(am) = af(m) \Rightarrow f(m) \in T(N)$. Dimostriamo ora che si tratta di una successione esatta.

   - $\overline{f}$ è iniettiva perchè restrizione di una mappa iniettiva;
   - $Ker\overline{g} \supseteq Im\overline{f}$ perchè $\forall m \in T(M)$ $(\overline{g} \circ \overline{f})(m) = (g \circ f)(m) = 0 \Rightarrow Im\overline{f} \subseteq Ker\overline{g}$;
   - $Ker\overline{g} \subseteq Im\overline{f}$ poichè $n \in Ker\overline{g} \Leftrightarrow \overline{g}(n) = g(n) = n \Rightarrow \exists n \in Imf \Leftrightarrow \exists m \in M \mid f(m) = n$; ma $n \in T(N) \Leftrightarrow \exists b \neq 0$ tale che $bn = 0 = bf(m) = f(bm)$, e per iniettività di f si conclude che $m \in T(M)$.

□

Concludiamo questa sezione con un esercizio.

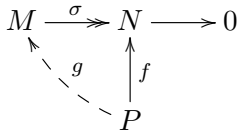
Esercizio (Esercizio 2.a, Giugno 2012)**.** Sia A PID e sia M modulo su A non finitamente generato e privo di torsione. Possiamo concludere che M sia libero?

La risposta è negativa, e il controesempio ci è dato da $\mathbb{Q}$ visto come modulo su $\mathbb{Z}$.

4.7 Moduli Proiettivi

Abbiamo dimostrato che Hom è esatto a sinistra. Ci proponiamo adesso dare delle condizioni sufficienti sui moduli affinchè tale funtore sia esatto anche a destra, e quindi esatto. A tal proposito introduciamo la seguente nozione.

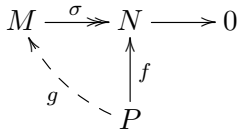
Definizione 4.7.1. *Siano A anello e M, N, P degli A-moduli, e sia $\sigma : M \longrightarrow N$ surgettiva. P si dice **proiettivo** se $\forall \phi \in Hom(P, N)$ $\exists g \in Hom(P, M)$ tale che $f = \sigma \circ g$, ovvero:*



è un diagramma commutativo.

Lemma 4.7.1. *Sia P modulo libero su un anello A. Allora P è proiettivo.*

Dimostrazione. Supponiamo di avere $M \xrightarrow{\sigma} N \longrightarrow 0$ successione esatta corta; vogliamo dimostrare che $\forall f \in Hom(P, N)$ $\exists g \in Hom(P, M)$ tale che $\sigma \circ g = f$. La situazione è la seguente:



Il nostro obiettivo è definire g. P è libero, quindi possiamo possiamo scegliere una sua base $\{e_i\}_{i \in I}$. Vogliamo che il diagramma commuti, e sappiamo che $f(e_i) = n_i$, quindi vorremmo scegliere un elemento $\sigma^{-1}(n_i)$ e porlo uguale a $g(e_i)$. Poichè P è libero, possiamo definire la mappa in questa maniera senza bisogno di ulteriori verifiche. □

Proposizione 4.7.1. *Siano M, N, P-moduli su A. Allora i seguenti fatti sono equivalenti:*

1. *P è proiettivo;*
2. *P è addendo diretto di un modulo libero;*

3. *ogni successione esatta corta del tipo* $0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0$ *spezza;*

4. *il funtore* Hom *è esatto.*

Dimostrazione. Facciamo vedere le varie implicazioni.

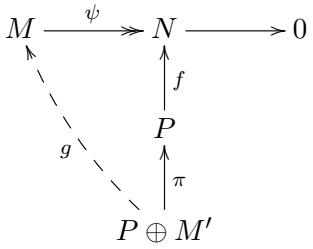
- (1) $\Leftrightarrow$ 4)) Segue direttamente dalla definizione di modulo proiettivo.

- (1) $\Rightarrow$ 3)) Sia $0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0$ esatta corta. Abbiamo dimostrato varie condizioni equivalenti al fatto che la successioni spezzi, tra le quali vi è il fatto che ψ ammetta una sezione $\alpha : P \longrightarrow N$, ovvero una mappa α tale che $\psi \circ \alpha = \mathrm{id}_P$. Guardiamo dunque la definizione di modulo proiettivo: se scegliamo $f = \mathrm{id}_P$, la mappa g altro non è che α.

- (3) $\Rightarrow$ 2)) Sia A^P modulo libero ottenuto prendendo tante copie di A quanti sono gli elementi di P. Allora $0 \longrightarrow Ker\pi \xrightarrow{i} A^P \xrightarrow{\pi} P \longrightarrow 0$ è esatta e spezza per ipotesi $\Rightarrow A^P \cong Ker\pi \oplus P$, quindi P è addendo diretto di un modulo libero.

A questo punto ci servirebbe dimostrare che 2) $\Rightarrow$ 1); in maniera equivalente, faremo vedere che 2) $\Rightarrow$ 4).

- (2) $\Rightarrow$ 4)) Supponiamo che P sia addendo diretto di un certo modulo libero $P \oplus M'$. Allora, se $f \in Hom(P, N)$, osserviamo che $\exists g \in Hom(P \oplus M', M)$ tale che il seguente diagramma commuti:



  Dunque $g \circ \psi = f \circ \pi$. Sia adesso $i : P \longrightarrow P \oplus M'$ l'omomorfismo di inlcusione; allora la mappa $g \circ i$ è quella che cercavamo, giacché $f \circ \pi \circ i = \psi \circ g \circ i = f$.

□

Capitolo 5

Anelli e Moduli di Frazioni

Sia A un anello e $S \subseteq A$ un suo sottoinsieme con la proprietà di essere moltiplicativamente chiuso, ovvero $1 \in S$ e $s, t \in S \Rightarrow st \in S$.
Alcuni esempi di sottoinsiemi moltiplicativamente chiusi sono

- $S = \{s^n\}_{n \in \mathbb{N}}, s \in A$
- $\mathfrak{p} \subseteq A, S = A - \mathfrak{p}$ è moltiplicativamente chiuso.

Consideriamo ora le coppie $(a, s) \in A \times S$ e affermiamo che $(a, s) \sim (b, t) \Leftrightarrow \exists u \in A \mid u(at - bs) = 0$ in A. Chiaramente, se $0 \in S$, allora ogni coppia è equivalente ad ogni altra, perciò d'ora in poi supporremo che $0 \notin S$. Ciò detto, osserviamo anche che se A è integro, la richiesta che esista u è superflua poichè $u(at - bs) = 0$ sarà soddisfatta quando $at - bs = 0$. Verifichiamo ora di aver definito una relazione d'equivalenza, così da poter lavorare con il quoziente.

- **Riflessiva:** basta scegliere $u = 1 \in S$;
- **Simmetrica:** $(a, s) \sim (b, t) \Leftrightarrow \exists u \in S \mid u(at - bs) = 0 \Rightarrow u(bs - at) = 0$;
- **Transitiva:** $(a, s) \sim (b, t),\ (b, t) \sim (c, v) \Leftrightarrow \exists u, w \in S \mid u(at - bs) = 0 = w(bv - ct) \Rightarrow uwt(at - cs) = 0$[1].

Consideriamo dunque $A \times S / \sim := S^{-1}A$, e indichiamo le sue classi come $[(a, s)] = \frac{a}{s}$. Vediamo ora che è possibile dotarlo della struttura di anello mediante le seguenti operazioni:

$$+ \quad \frac{a}{t} + \frac{b}{s} = \frac{at + bs}{st}$$

$$\cdot \quad \frac{a}{t} \cdot \frac{b}{t} = \frac{ab}{st}$$

[1] A breve aggiungerò il conto per esteso – abbiate pazienza!

Ovviamente, per darvi motivo di odiarmi almeno un po', non verificherò (per ora) che siano ben definite; ve lo lascio per esercizio[2].
Con questa struttura, $S^{-1}A$ è detto *Anello delle Frazioni* di A rispetto ad S.

Esempio. Se $A = \mathbb{Z}$ e $S = \{6^n\}_{n\in\mathbb{N}}$ allora $S^{-1}A = \{\frac{a}{6^n} \mid a \in \mathbb{Z}\} \subseteq \mathbb{Q}$. Se invece scegliamo $S\mathbb{Z} - \mathfrak{p} \Rightarrow S^{-1}A = \{\frac{a}{s} \mid a \in \mathbb{Z} \wedge s \notin \mathfrak{p}\}$.

Vediamo ora una prima naturale mappa tra l'anello delle frazioni di un certo anello e l'anello stesso.

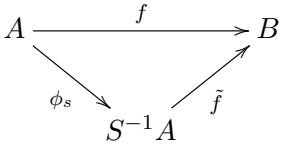
$$\begin{aligned} \phi_s : A &\longrightarrow S^{-1}A \\ a &\longrightarrow \frac{a}{1} \end{aligned}$$

In generale non si tratta di una mappa iniettiva: $\phi_a(a) = 0 \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists u \in S \mid ua = 0$, da cui, sempre nell'ipotesi in cui $0 \notin S$, segue che $S \cap D(A) \neq \emptyset$. Se invece A è un dominio, la mappa è iniettiva.
Adesso cercheremo di capire meglio come sia fatto l'anello delle frazioni rispetto ad un sottoinsieme. Per ora possiamo osservare con facilita che se $s \in S \Rightarrow \frac{s}{1}$ è invertibile in $S^{-1}A$, quindi abbiamo sicuramente invertito tutti gli elementi di S.

Osservazione. Nel caso in cui A non sia un dominio, se localizziamo rispetto ad $S \subseteq A$ sottoinsieme moltiplicativamente chiuso che interseca i divisori di zero, allora nella classe di equivalenza di 0 rientreranno molti più elementi. Infatti, se $u \in S \cap D(A)$, allora $\frac{0}{1} = \frac{a}{t}$ ogni volta che $ua = 0$. In altri termini, se $u \in A \cap S$, allora $\phi_s(Ann(u)) = 0$.

Enunciamo ora, e dimostriamo, la Proprietà Universale dell'Anello delle Frazioni.

Proposizione 5.0.1 (Proprietà Universale dell'Anello delle Frazioni)**.** *Sia $A \xrightarrow{f} B$ un omomorfismo di anelli e sia $S \subseteq A$ moltiplicativamente chiuso. Se $f(S) \subseteq B^* \Rightarrow \exists! \tilde{f} : S^{-1}A \longrightarrow B$ tale che il seguente diagramma commuti:*



Dimostrazione. Cominciamo con l'unicità. Se esiste $\tilde{f}$, allora $\tilde{f}(\frac{1}{s}) = (\tilde{f}(\frac{s}{1}))^{-1} = f(s)^{-1}$, che ha senso perchè $f(S) \subseteq B^*$. Allora necessariamente $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$, quindi è unica.
Sia dunque $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$; vediamo che è ben definita. $\tilde{f}(\frac{a}{s}) = \tilde{f}(\frac{b}{t}) \Leftrightarrow \exists u \in S$ tale che $u(at-bs) = 0 \Rightarrow f(u)(f(a)f(t)-f(b)f(s)) = 0 \Leftrightarrow f(a)f(t) = f(b)f(s) \Leftrightarrow f(a)f(s)^{-1} = f(b)f(t)^{-1}$. □

[2]Non avete idea dell'emozione che provo nello scrivere per la prima volta questa cosa.

Proposizione 5.0.2. *Sia $A \xrightarrow{f} B$ un omomorfismo di anelli e sia $S \subseteq A$ moltiplicativamente chiuso. Se f è tale che:*

- *$f(S) \subseteq B^*$;*
- *$f(a) = 0 \Rightarrow \exists n \in S \mid na = 0$;*
- *$\forall b \in B \mid b = f(a)f(s)^{-1}$;*

allora $\tilde{f}$ è isomorfismo.

Dimostrazione. $\tilde{f}(\frac{a}{s}) = \frac{0}{1} = f(a)f(s)^{-1} \Rightarrow f(a) = 0 \Leftrightarrow \exists u \in S \mid ua = 0 \Rightarrow \frac{a}{s} = \frac{0}{1}$ poichè $u(a \cdot 1 - s \cdot 0) = ua = 0$, dunque $\tilde{f}$ è iniettiva. La surgettività altro non è che la seconda ipotesi. □

Vediamo ora due interessanti Anelli di Frazioni.
Se $A = \mathbb{Z}$ e $S = \{a^n\}$, allora $S^{-1}A = \mathbb{Z}_{(a)} = \{\frac{b}{a^n} \mid b \in \mathbb{Z}, n \in \mathbb{N}\}$. Se invece scegliamo $\mathfrak{p} = (p) \subseteq \mathbb{Z}$ e $S = \mathbb{Z} - \mathfrak{p}$, allora $S^{-1}A = \mathbb{Z}_p = \{\frac{a}{s} \mid s \notin (p)\}$.
Di questi anelli ci interessa particolarmente $\mathbb{Z}_p$, poichè è *locale* con ideale massimale (p). In generale, se $P \subseteq A$ è un primo, l'anello A_P è locale con massimale $\mathfrak{m} = \{\frac{a}{s} \mid a \in P, s \notin P\}$[3].

5.1 Ideali di $S^{-1}A$

In questa sezione cercheremo di mettere in relazione ideali estesi e contratti tramite la mappa $\phi_s : A \longrightarrow S^{-1}A$. Per ora possiamo cominciare osservando che $\forall I \subseteq A$ ideale abbiamo $(\phi_s(I)) = \{\sum \frac{a_i}{s_i}\frac{b_i}{1} \mid a_i \in A, s_i \in S\}$, ma $\sum \frac{a_i}{s_i}\frac{b_i}{1} = \sum \frac{t_i a_i b_i}{s}$, dove $s = \prod s_i$ e $t_i = \prod_{j \neq i} s_j$, quindi $I^e = (\phi_s(I)) \subseteq S^{-1}I$.
Quello che vedremo adesso, insieme ad altri risultati, è che effettivamente vale anche l'altra inclusione, ovvero tutti gli ideali di $S^{-1}A$ sono ideali estesi.

Proposizione 5.1.1. *Sia A anello, S un suo sottoinsieme moltiplicativamente chiuso; consideriamo $S^{-1}A$. Allora valgono le seguenti affermazioni:*

1. *ogni ideale di $S^{-1}A$ è estensione di un ideale di A;*
2. *$\forall I \subseteq A$ ideale, $I^{ec} = \bigcup_{s \in S} (I : s)$;*
3. *c'è una corrispondenza biunivoca tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A che non intersecano S.*

Dimostrazione. Vediamo il primo punto. In generale è vero che $J^{ce} \subseteq J$, ma in questo caso vale anche l'altra inclusione:

$$\frac{a}{t} \in J \Rightarrow \frac{t}{1}\frac{a}{t} = \frac{a}{1} \in J \Rightarrow a \in J^c \Rightarrow \frac{a}{t} = \frac{a}{1}\frac{1}{t} \in J^{ce}.$$

[3]Prossimamente aggiungerò una dimostrazione di questo fatto.

Passiamo al secondo. Per quanto appena visto, se $I^{ec} = (S^{-1}I)^c$. Sia ora $\alpha \in I^{ec}$, $\phi_s(\alpha) = \frac{\alpha}{1} \in I^e = S^{-1}I$, dunque $\frac{\alpha}{1} = \frac{a}{s} \Leftrightarrow \exists u \in S \mid u\alpha s = ua \in I \Rightarrow \alpha \in (I : (us))$. Viceversa, sia $\alpha \in (I : t), t \in S \Rightarrow at \in I \Rightarrow \frac{at}{1} \in S^{-1}I$, da cui $\frac{at}{t} = \frac{a}{1} = \phi_s(a) \in S^{-1}I$, ovvero $a \in I^{ec}$.
Per dimostrare il terzo punto consideriamo la seguente mappa:

$$\begin{aligned} \{\mathfrak{p} \in Spec(A) \mid \mathfrak{p} \cap S = \emptyset\} &\longrightarrow Spec(S^{-1}A) \\ \mathfrak{p} &\longmapsto S^{-1}\mathfrak{p} \end{aligned}$$

La mappa è ben definita se l'estensione di un ideale primo tramite ϕ_s è ancora un ideale primo; verifichiamolo. Sia $\mathfrak{p} \in Spec(A)$ tale che $\mathfrak{p} \cap S = \emptyset$ e sia $\frac{a}{s}\frac{b}{t} \in S^{-1}\mathfrak{p} \Leftrightarrow \frac{ab}{st} = \frac{p}{r} \Leftrightarrow \exists u \in S$ tale che $uabr = upst \in \mathfrak{p}$; ma $u, s, t, r \in S \Rightarrow u, s, t, r \notin \mathfrak{p}$, quindi per primalità segue che $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p} \Rightarrow \frac{a}{s} \in S^{-1}\mathfrak{p} \vee \frac{b}{t} \in S^{-1}\mathfrak{p}$.
Ciò detto, verifichiamo che la mappa sia bigettiva.

- Surgettività: sia $P \in Spec(S^{-1}A) \Rightarrow P = S^{-1}P^c$; poichè la contrazione di un ideale primo è sempre un ideale primo, dobbiamo solo assicurarci che $P^c \cap S = \emptyset$. Ma se, per assurdo, $P^c \cap S \neq \emptyset \Rightarrow S^{-1}P = S^{-1}A$, che è chiaramente assurdo perchè nella definizione di ideale primo richiediamo che sia anche un ideale proprio.

- Iniettività: supponiamo che $S^{-1}P_1 = S^{-1}P_2$, allora $\forall a \in P_1\ \exists \frac{b}{t} \in S^{-1}P_2 \mid \frac{a}{1} = \frac{b}{t} \Leftrightarrow \exists u \in S \mid uat = ub \in P_2$. Poichè per ipotesi $P_1 \cap S = \emptyset = O_2 \cap S$, segue che $a \in P_2$. Allo stesso modo si ottiene l'altra inclusione, da cui l'uguaglianza.

□

Quindi ogni ideale $J \subseteq S^{-1}A$ altro non è che $S^{-1}J^c$.

Vediamo ora quali operazioni tra ideali possiamo gestire con facilità quando passiamo all'anello delle frazioni.

Proposizione 5.1.2. *Sia A anello, S un suo sottoinsieme moltiplicativamente chiuso e I, J due generici ideali. Allora S^{-1} commuta con somma e intersezione finita, e con il radicale, ovvero:*

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

Dimostrazione. In tutti i casi facciamo vedere le due inclusioni.

– $(\subseteq)$ $S^{-1}(I + J) \ni \frac{i+j}{s} = \frac{is+js}{s^2} = \frac{i}{s} + \frac{j}{s} \in S^{-1}I + S^{-1}J$.

- $(\supseteq)$ $S^{-1}I + S^{-1}J \ni \frac{i}{s} + \frac{j}{t} = \frac{ti+sj}{ts} \in S^{-1}(I+J)$.

- $(\subseteq)$ $S^{-1}I \cap S^{-1}J \ni \frac{h}{s}, h \in I \cap J \Rightarrow \frac{h}{s} = \frac{i}{t} = \frac{j}{u},\ i \in I,\ j \in J$, da cui $\exists w \in S \mid wiu = wjt \in I \cap J \Rightarrow \frac{i}{t} = \frac{wiu}{wut} \in S^{-1}(I \cap J)$.
- $(\supseteq)$ $S^{-1}(I \cap J) \ni \frac{h}{s}$, $h \in I \cap J \Rightarrow \frac{h}{s} \in S^{-1}I \cap S^{-1}J$.

- $(\subseteq)$ $S^{-1}\sqrt{I} \ni \frac{a}{t} \Leftrightarrow \exists n \in \mathbb{N} \mid a^n \in I \Rightarrow \frac{a^n}{t^n} = \frac{a^n}{t} \cdot \frac{1}{t^{n-1}} \in S^{-1}I \Rightarrow \frac{a}{t} \in \sqrt{S^{-1}I}$.
- $(\supseteq)$ $\sqrt{S^{-1}I} \ni \frac{a}{t} \Leftrightarrow \exists n \in \mathbb{N} \mid \frac{a^n}{t^n} \in S^{-1}I \Leftrightarrow \frac{a^n}{t^n} = \frac{i}{s} \in S^{-1}I \Leftrightarrow \exists u \in S$ tale che $ua^n s = it^n$, da cui $(uas)^n \in I \Rightarrow uas \in \sqrt{I} \Rightarrow \frac{uas}{1} \in S^{-1}\sqrt{I} \Rightarrow \frac{uas}{1} \cdot \frac{1}{ust} = \frac{a}{t} \in S^{-1}\sqrt{I}$.

□

Arrivati a questo punto, è naturale voler accostare questa nuova struttura con degli opportuni moduli. Se dunque M è un A-modulo, consideriamo $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso e introduciamo su $M \times S$ una relazione di equivalenza analoga a quella vista nel caso di un anello A, ovvero diciamo che $(m,t) \sim (n,t) \Leftrightarrow \exists s \in S \mid u(mt - ns) = 0$. Con questa relazione e con le seguenti operazini otteniamo il modulo $S^{-1}M$ sull'anello $S^{-1}A$.

$$+ \quad \frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$$

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

Le verifiche sono lasciate ai più diligenti.

Prima di addentrarci nella selva degli ideali di $S^{-1}A$ e in tutta una serie di fantastici conti, cercheremo di far fruttare l'impegno messo fino ad ora nella definizione di queste nuove strutture osservandole da un particolare punto di vista: dimostreremo che S^{-1} è un *funtore esatto*.

Proposizione 5.1.3. *Il funtore S^{-1} è esatto, ovvero trasforma successioni esatte in successioni esatte.*

Dimostrazione. Siano M, N, P moduli su A e siano $f : M \longrightarrow N$ e $g : N \longrightarrow P$ omomorfismi di A moduli tali che la seguente sia una successione esatta:

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

Vogliamo dimostrare che anche la successione

$$0 \longrightarrow S^{-1}M \xrightarrow{\tilde{f}} S^{-1}N \xrightarrow{\tilde{g}} S^{-1}P \longrightarrow 0$$

dove $\tilde{f}(\frac{m}{s}) = \frac{f(m)}{s}$ e $\tilde{g}(\frac{n}{s'}) = \frac{g(n)}{s'}$, è anch'essa esatta.

- $\tilde{f}$ è iniettiva perchè $ker\tilde{f} = \{\frac{m}{s} \in S^{-1}M \mid \tilde{f}(\frac{m}{s}) = 0\}$, ma $\tilde{f}(\frac{m}{s}) = \frac{f(m)}{s} = \frac{0}{1}$ se e soltanto se $\exists u \in S \mid uf(m) = 0 \Leftrightarrow f(um) = 0 \Leftrightarrow um = 0 \Rightarrow \frac{m}{s} = \frac{0}{1} \in S^{-1}M$.
- $\tilde{g}$ è surgettiva perchè $\forall p \in P \ \exists n \in N$ tale che $g(n) = p$, quindi $\forall \frac{p}{n} \in S^{-1}P \ \exists \frac{n}{s} \in S^{-1}N \mid \tilde{g}(\frac{n}{s}) = \frac{g(n)}{s} = \frac{p}{s}$.

Per quanto riguarda $Ker\tilde{g} = Im\tilde{f}$, facciamo vedere le due inclusioni.

($\subseteq$) Sia $\frac{n}{s} \in ker\tilde{g} \Leftrightarrow \frac{g(n)}{s} = \frac{0}{1} \in S^{-1}P \Leftrightarrow \exists u \in S$ tale che $ug(n) = 0 \Leftrightarrow g(un) = 0 \Leftrightarrow un \in Kerg = Imf \Leftrightarrow \exists m \in M \mid f(m) = un \Rightarrow \frac{n}{s} = \frac{un}{us} = \frac{f(m)}{us} = \tilde{f}(\frac{m}{us}) \in Im\tilde{f}$.

($\supseteq$) $\forall \frac{\tilde{m}}{s} \in Im\tilde{f}, \tilde{f}(\frac{m}{s}) = \frac{f(m)}{s}$, quindi $\tilde{g}(\frac{f(m)}{s}) = \frac{g(f(m))}{s} = \frac{0}{1}$.

□

Dotati di questo strumento, possiamo dimostrare con facilità la seguente proposizione.

Proposizione 5.1.4. *S^{-1} commuta con l'operazione di quoziente, ovvero se M, N sono sottomoduli di un modulo P e $N \subseteq M$, allora $S^{-1}(M\,/\,N) = S^{-1}M\,/\,S^{-1}N$.*

Dimostrazione. Consideriamo le seguenti successioni esatte.

$$0 \longrightarrow N \longrightarrow M \longrightarrow {}^{M}/_{N} \longrightarrow 0$$

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

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

Vorremmo applicare il lemma dei cinque alle ultime due, dobbiamo dunque definire una mappa tra $S^{-1}M\,/\,S^{-1}N$ e $S^{-1}(M\,/\,N)$ che faccia commutare il diagramma, poichè come altre mappe possiamo considerare l'identità.
Sia allora

$$\begin{aligned} \gamma : S^{-1}({}^{M}/_{N}) &\longrightarrow {}^{S^{-1}M}/_{S^{-1}N} \\ \frac{m+N}{s} &\longmapsto \frac{m}{s} + S^{-1}N \end{aligned}$$

Questa mappa è ben definita perchè se $m + N = m + n + N$, allora $\frac{m+n}{s} + S^{-1}N = \frac{m}{s} + S^{-1}N$.
Specifichiamo inoltre che la mappa tra $S^{-1}M$ e $S^{-1}(M\,/\,N)$ è $\tilde{\pi}(\frac{m}{s}) = \frac{\pi(m)}{s}$, con $\pi : M \longrightarrow M\,/\,N$.
Si verifica facilmente che queste mappe rendono il diagramma commutativo, quindi, per il Lemma dei Cinque, si ha l'isomorfismo cercato. □

Abbiamo visto come si comporta S^{-1} rispetto alla somma, all'intersezione, al radicale, e al quoziente; vediamo cosa succede se consideriamo il colon di ideali o moduli.

In generale, si verifica facilmente che se M, N sono sottomoduli di un modulo P, allora $S^{-1}(M : N) \subseteq S^{-1}M : S^{-1}N$, e non sempre vale l'uguale; con delle ipotesi aggiuntive, però, abbiamo l'uguaglianza.

Proposizione 5.1.5. *Siano M, N sottomoduli di un modulo P. Se N è finitamente generato, allora $S^{-1}(M : N) = S^{-1}M : S^{-1}N$.*

Dimostrazione. Vediamo le due inclusioni.

($\subseteq$) $S^{-1}(M : N) = \{\frac{h}{s} \mid h \in (M : N), s \in S\}$, quindi $\forall n \in N\ nh \in M \Rightarrow \forall \frac{n}{u} \in S^{-1}N$ si ha che $\frac{h}{s} \cdot \frac{n}{u} = \frac{nh}{ut} \in S^{-1}M$, da cui $\frac{h}{t} \in (S^{-1}M : S^{-1}N)$.

($\supseteq$) Dimostriamolo per induzione sul numero di generatori. Se $N =< n >$, allora consideriamo $\psi : A \longrightarrow N \mid a \mapsto an_1$ e osserviamo che $Ker\psi = Ann(N)$. Per esattezza del funtore S^{-1} abbiamo due successioni esatte corte:

$$0 \longrightarrow Ann(N) \longrightarrow A \longrightarrow N \longrightarrow 0$$

$$0 \longrightarrow S^{-1}(Ann(N)) \longrightarrow S^{-1}A \longrightarrow S^{-1}N \longrightarrow 0$$

ma anche

$$0 \longrightarrow Ann(S^{-1}N) \longrightarrow S^{-1}A \longrightarrow S^{-1}N \longrightarrow 0$$

Quindi $Ann(S^{-1}N)$ e $S^{-1}(Ann(N))$ sono il nucleo della medesima mappa.
Nel caso di n generatori, sfruttiamo le proprietà del'annullatore e osserviamo che se scriviamo $N = N_1 + N_2$, con N_1, N_2 generati da un numero di elementi minore stretto di n, allora

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

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

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

□

Vediamo, per completezza, un caso nel quale non vale l'uguaglianza. Scegliamo $A = \mathbb{K}[x, t, \frac{x}{t}, \frac{x}{t^2}, \cdots]$ e $S = \{t^n\}_{n\in\mathbb{N}}$. Consideriamo gli ideali $I = (x)$ e $J = (\frac{x}{t}, \frac{x}{t^2}, \cdots)$. Osserviamo che $I : J = I$, da cui $S^{-1}(I : J) = S^{-1}I$. Quando invece calcoliamo $(S^{-1}I : S^{-1}J)$ otteniamo $S^{-1}A$ poichè $S^{-1}I$ contiene $S^{-1}J$, infatti

$$\forall\ \frac{\frac{x}{t^k}}{1} \in S^{-1}J, \quad \frac{\frac{x}{t^k}}{1} = \frac{x}{t^k}$$

poichè

$$\forall h \in \mathbb{N} \quad t^h x = t^h(t^k \cdot \frac{x}{t^k}).$$

5.2 Proprietà Locali

In questa sottosezione vedremo delle proprietà dette *locali* in quanto verificano l'equivalenza P vera in M modulo su $A \Leftrightarrow \forall \mathfrak{p}$ ideale primo di A, P è vera in $M_{\mathfrak{p}}$.

Proposizione 5.2.1. *Sia M un A-modulo. Le seguenti affermazioni sono equivalenti.*

1. $M = 0$;
2. $M_{\mathfrak{p}} = 0\ \forall \mathfrak{p}$ *ideale primo di* A;
3. $M_{\mathfrak{m}} = 0\ \forall \mathfrak{m}$ *ideale massimale di* A.

Dimostrazione. Chiaramente 1) $\Rightarrow$ 2) $\Rightarrow$ 3). Dobbiamo dunque mostrare che 3) $\Rightarrow$ 1). $\forall \mathfrak{m} \subseteq A, M_{\mathfrak{m}} = 0 \Leftrightarrow \forall \frac{m}{t} \in M_{\mathfrak{m}}, \frac{m}{t} = \frac{0}{1} \Leftrightarrow \exists u \notin \mathfrak{m}$ tale che $um = 0$. Da questo deduciamo che $Ann(M) \not\subseteq \mathfrak{m}\ \forall \mathfrak{m} \subseteq A$, quindi $Ann(M) = A \Rightarrow M = 0$. □

Proposizione 5.2.2. *Sia $\phi : M \longrightarrow N$ omomorfismo di A-moduli. Le seguenti affermazioni sono equivalenti.*

1. ϕ *è iniettivo;*
2. $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ *è iniettivo* $\forall \mathfrak{p}$ *ideale primo di* A;
3. $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ *è iniettivo* $\forall \mathfrak{m}$ *ideale massimale di* A.

Dimostrazione. 1) $\Rightarrow$ 2) perchè il funtore S^{-1} è esatto; e 2) $\Rightarrow$ 3) perchè tutti i massimali sono anche primi. Resta da dimostrare 3) $\Rightarrow$ 1).
Sia $\phi(a) = 0 \in M \Rightarrow \forall \mathfrak{m} \subseteq A$ vale $\phi_{\mathfrak{m}}(\frac{a}{1}) = \frac{\phi(a)}{1} = \frac{0}{1} \Leftrightarrow \frac{a}{1} = \frac{0}{1}$ per iniettività di $\phi_{\mathfrak{m}}$. Allora $\forall \mathfrak{m} \subseteq A \exists u \notin \mathfrak{m} \mid ua = 0$, per cui $(0 : a) = A$ e $a = 0$. □

Proposizione 5.2.3. *Sia $\phi : M \longrightarrow N$ omomorfismo di A-moduli. Le seguenti affermazioni sono equivalenti.*

1. *ϕ è sugettiva;*
2. *$\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ è surgettiva $\forall \mathfrak{p}$ ideale primo di A;*
3. *$\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ è surgettiva $\forall \mathfrak{m}$ ideale massimale di A.*

Dimostrazione. Come prima, 1) $\Rightarrow$ 2) per esattezza di S^{-1} e 2) $\Rightarrow$ 3) perchè ogni massimale è anche primo. Facciamo vedere che 3) $\Rightarrow$ 1). $\forall \mathfrak{m} \subseteq A, \phi_{\mathfrak{m}}$ è surgettiva, e poichè $\forall \frac{m}{t} \in S^{-1}M . \phi_{\mathfrak{m}}(\frac{m}{t}) = \frac{\phi(m)}{t}$, la surgettività è equivalente a dire che $\forall n \in N \ \exists \frac{m}{t} \in S^{-1}M$ tale che $\phi_{\mathfrak{m}}(\frac{m}{t}) = \frac{\phi(m)}{t}\frac{n}{1} \Leftrightarrow \exists u \notin \mathfrak{m}$ tale che $u\phi(m)\phi(um) = unt$. Da questo deduciamo che $(Im\phi : N) \not\subseteq \mathfrak{m}$ per ogni $\mathfrak{m}$ in A, da cui $(Im\phi : N) = (1) \Leftrightarrow Im\phi = N$. □

Esercizio. Essere dominio è una proprietà locale? Essere ridotto è una proprietà locale?

L'integrità non è una proprietà locale. Consideriamo infatti $\mathbb{Z} \times \mathbb{Z}$: localmente non solo è integro, ma è anche un campo, tuttavia sappiamo che il prodotto di domini non è integro. Un altro controesempio, come al solito, ci è dato dal nostro carissimo $\mathbb{Z}/(6)$.
É invece vero che la proprietà di essere ridotto sia locale. Essenzialmente, segue dal fatto che S^{-1} commuti con il radicale, però vediamo nello specifico come si dimostra.

Proposizione 5.2.4. *(Facoltativo) Sia A anello.*

$$A \text{ è ridotto } \Leftrightarrow \ \forall \mathfrak{p} \subseteq A \ A_{\mathfrak{p}} \text{ è ridotto}$$

Dimostrazione. ($\Rightarrow$) Sia A ridotto e sia $\frac{a}{s} \in A_{\mathfrak{p}}$ nilpotente, ovvero

$$\exists n \in \mathbb{N} \mid \frac{a^n}{s^n} = \frac{0}{1} \Leftrightarrow \exists t \notin \mathfrak{p} \mid ta^n = 0 = (ta)^n.$$

A è ridotto, quindi $at = 0 \Rightarrow a = 0$, perchè $Ann(a) \not\subseteq \mathfrak{p} \ \forall \mathfrak{p}$.

($\Leftarrow$) Supponiamo che $A_{\mathfrak{p}}$ sia ridotto per ogni ideale primo $\mathfrak{p}$ e prendiamo $a \in N(A)$. Esisterà $n \in \mathbb{N}$ tale che $a^n = 0 \Rightarrow \forall \mathfrak{p} \subseteq A \ \frac{a^n}{1} = \frac{0}{1}$; ma $A_{\mathfrak{p}}$ è ridotto $\Rightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists t_{\mathfrak{p}} \notin \mathfrak{p} \mid t_{\mathfrak{p}}a = 0$. Osserviamo ora che $(0 : a) \not\subseteq \mathfrak{p} \ \forall \mathfrak{p} \subseteq A \Rightarrow (0 : a) = A \Rightarrow 1 \in (0 : a) \Rightarrow a = 0$.

□

Un risultato analogo, anche nella dimostrazione, a quello appena visto, è il seguente.

Proposizione 5.2.5. *(Facoltativo) Sia I ideale di un anello A. Allora*

$$I = \sqrt{I} \Leftrightarrow \ \forall \mathfrak{p} \subseteq A \ I_{\mathfrak{p}} = \sqrt{I_{\mathfrak{p}}}.$$

Dimostrazione. ($\Rightarrow$) Sia $I = \sqrt{I}$ e sia $\mathfrak{p}$ un qualsiasi ideale primo in A. Sappiamo che in generale $I \subseteq \sqrt{I}$, quindi mostreremo solo l'inclusione opposta.

$$\frac{a}{t} \in \sqrt{I_{\mathfrak{p}}} \Leftrightarrow \exists n \in \mathbb{N} \mid \frac{a^n}{t^n} \in I_{\mathfrak{p}}$$

Sappiamo però che $\forall J \subseteq S^{-1}A \ J = s^{-1}J^c$, ovvero $J = J^{ce}$, quindi

$$\frac{a^n}{t^n} = \frac{b}{1} \in I_{\mathfrak{p}}, \ b \in I \Leftrightarrow \exists u \notin \mathfrak{p} \mid ua^n = ubt^n \in I$$

$$\Rightarrow ua^n \in I \Rightarrow (ua)^n \in I = \sqrt{I} \Rightarrow ua \in I \Rightarrow a \in I$$

poichè se $u \in I \Rightarrow \mathfrak{p} \cap I \neq \emptyset \Rightarrow S^{-1}I = I_{\mathfrak{p}} = S^{-1}A$.

($\Leftarrow$) Sia $a \in \sqrt{I} \Leftrightarrow \exists n \in \mathbb{N} \mid a^n \in I$. Allora

$$\frac{a^n}{1} \in I_{\mathfrak{p}} = \sqrt{I_{\mathfrak{p}}} \Rightarrow \frac{a^n}{1} = \frac{b}{1} \in \sqrt{I_{\mathfrak{p}}} \Leftrightarrow \exists t_{\mathfrak{p}} \notin \mathfrak{p} \mid t_{\mathfrak{p}}a = t_{\mathfrak{p}}b \in I$$

Quindi, come nell'esercizio precedente, possiamo osservare che

$$(I : a) \not\subseteq \mathfrak{p} \ \forall \mathfrak{p} \subseteq A \Rightarrow (I : a) = A \Leftrightarrow 1 \in (I : a) \Rightarrow a \in I.$$

□

Questa proposizione si può anche dimostrare sfruttando l'equivalenza I primo $\Leftrightarrow A/I$ integro, e riducendosi a lavorare con i nilpotenti. Effettivamente, ragionando come nei casi precedenti si può dimostrare che la proprietà di essere radicale è locale. Nella proposizione è riportata solo l'equivalenza nel caso di localizzazione per primi perchè in questo modo era formulato un esercizio di un vecchio compito.

Con una dimostrazione del tutto analoga a quelle appena viste si arriva a far vedere che anche la seguente è una proprietà locale. Per ora lo enunciamo come esercizio e lasciamo al lettore lo svolgimento della sua dimostrazione.

Esercizio. Sia M modulo su A. Allora le seguenti sono equivalenti.

1. M è libero da torsione.
2. $\forall \mathfrak{p} \subseteq A \ M_{\mathfrak{p}}$ è libero da torsione.
3. $\forall \mathfrak{m}$ ideale massimale in $A \ M_{\mathfrak{m}}$ è libero da torsione.

5.3 Unità in $S^{-1}A$

Cercheremo ora di far chiarezza riguardo a quali elementi vengano effettivamente invertiti quando passiamo all'anello delle frazioni rispetto ad un sottoinsieme moltiplicativamente chiuso. Questa necessità nasce da osservazioni come la seguente.

Osservazione. Nel passaggio da $\mathbb{Z}$ a $\mathbb{Z}_6$ quel che facciamo è invertire tutte le potenze di 6, ma effettivamente invertiamo anche 2 e 3, infatti: $\frac{3}{1} \cdot \frac{2}{6} = \frac{1}{1}$.

Per raggiungere il nostro obiettivo sarà necessario introdurre, come spesso accade, delle nuove definizioni.

Definizione 5.3.1. *Un sottoinsieme moltiplicativamente chiuso T di A si dice* ***saturato*** *se $st \in T \Rightarrow s \in T \wedge t \in T$.*

Avrete sicuramente intuito il seguente risultato:

Proposizione 5.3.1 (Caratterizzazione di Insiemi Saturati)**.** *Sia T un sottoinsieme moltiplicativamente chiuso di A anello. Allora T è saturato $\Leftrightarrow T = A - \bigcup \mathfrak{p}$*

Dimostrazione. Facciamo vedere le due implicazioni.

($\Leftarrow$) Sia T complementare dell'unione di ideali primi. Ogni ideale primo, per definizione, è un ideale proprio, quindi $1 \in T$. Siano ora $a, b \in T$. Se supponiamo che ab non stia in T giungiamo ad assurdo:

$$ab \notin T \Leftrightarrow \exists \mathfrak{p} \mid ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}.$$

Infine, se $ab \in T$ e per assurdo $\exists \mathfrak{p}$ nel complementare di T che contiene a, allora, poichè gli ideali sono chiusi rispetto alla moltiplicazione, $ab \in \mathfrak{p}$, che è assurdo.

($\Rightarrow$) Sia ora T saturato; vogliamo far vedere che è il complementare dell'unione di certi ideali primi dell'anello A. Affermiamo che

$$T = A - \bigcup_{\mathfrak{p} \cap T = \emptyset} \mathfrak{p}.$$

Facciamo vedere le due inclusioni.
($\subseteq$) Sia $t \in T \Rightarrow t \notin \mathfrak{p}$ $\forall \mathfrak{p}$ tale che $\mathfrak{p} \cap T = \emptyset$.
($\supseteq$)

□

Si verifica inoltre con facilità che $T = \{a \in A \mid \frac{a}{1} \text{ è invertibile in } T^{-1}A\}$.

A questo punto vorremmo dare la nozione di saturato di un insieme.

Proposizione 5.3.2. *Sia S un sottoinsieme moltiplicativamente chiuso di A anello e sia $\overline{S} = \{a \in A \mid \exists b \in A$ tale che $ab \in S\}$. Allora valgono le seguenti affermazioni:*

1. *$S \subseteq \overline{S}$;*
2. *$\overline{S}$ è saturato e moltiplicativo;*
3. *se T è moltiplicativo e saturato tale che $T \supseteq S \Rightarrow T \supseteq \overline{S}$;*
4. *$(S^{-1}A)^* = \{\frac{a}{s} \mid a \in \overline{S}, s \in S\}$;*
5. *$\overline{S} = A - \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$;*
6. *$S^{-1}A = \overline{S}^{-1}A$*

Dimostrazione. 1. $\forall s \in S, s \in \overline{S}$ perchè $s = 1 \cdot s \in S$.

2. Dimostriamo che $\overline{S}$ è moltiplicativo: $1 \in S \subseteq \overline{S}$; se $a, b \in \overline{S} \Leftrightarrow \exists a', b' \in A$ tali che $aa' \in A$ e $bb' \in S$, da cui $aa'bb' = (ab)a'b' \in S \Rightarrow ab \in \overline{S}$. Verifichiamo adesso che $\overline{S}$ è saturato: $ab \in \overline{S} \Leftrightarrow \exists c \in A$ tale che $abc \in S \Rightarrow a(bc) = b(ac) \in S \Rightarrow a, b \in \overline{S}$.

3. Sia T moltiplicativo e saturato tale che $T \supseteq S$ e sia $a \in \overline{S} \Leftrightarrow \exists b \in A$ tale che $ab \in S \subseteq T \Rightarrow a \in T \wedge b \in T$.

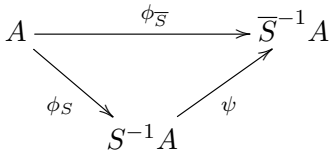
4. $\frac{a}{t} \in (S^{-1}A)^* \Leftrightarrow \exists \frac{b}{s} \in S^{-1}A$ tale che $\frac{ab}{st} = \frac{1}{1} \Leftrightarrow \exists u \in S \mid uab = 1 \in S \subseteq \overline{S} \Rightarrow u, a, b \in \overline{S}$, quindi se $\frac{a}{t}$ è invertibile allora $a \in \overline{S}$ e $t \in S$.

5. Cominciamo osservando che

$$\bigcup_{\mathfrak{p} \cap \overline{S} = \emptyset} \mathfrak{p} \subseteq \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p} \Rightarrow A - \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p} \subseteq A - \bigcup_{\mathfrak{p} \cap \overline{S} = \emptyset} \mathfrak{p} = \overline{S}$$

   Dimostriamo ora l'altra inclusione. Sia $s \in \overline{S} \Leftrightarrow \exists a \in A$ tale che $as \in S \Rightarrow as \notin \mathfrak{p}\ \forall \mathfrak{p}$ tale che $\mathfrak{p} \cap S = \emptyset \Rightarrow a \notin \mathfrak{p}$ per ognuno dei primi che non intersecano S, poichè siamo in presenza di ideali.

6. Consideriamo il seguente diagramma:



   Osserviamo, innenzitutto, che questo diagramma ha ragion d'essere perchè $\phi_{\overline{S}}(S) \subseteq (\overline{S}^{-1}A)^*$ per il punto precedente. Ora facciamo vedere che ψ è un isomorfismo.

- ψ è iniettiva se $\forall a \in A$ tale che $\phi_{\overline{S}}(a) = \frac{a}{1} = \frac{0}{1}$ esiste $s \in S$ tale che $sa = 0$; ma se $\frac{a}{1} = \frac{0}{1} \in \overline{S}^{-1}A \Leftrightarrow \exists s \in \overline{S}$ tale che $sa = 0$. $s \in S \Leftrightarrow \exists s' \in A \mid ss' \in S \Rightarrow ss'a = 0$, quindi $\frac{a}{1} = \frac{0}{1} \in S^{-1}A$.
- ψ è surgettiva perchè se $\frac{a}{t} \in \overline{S}^{-1}A \Rightarrow \exists u \in A$ tale che $ut \in S$, quindi $\frac{a}{t} = \frac{au}{tu} \in S^{-1}A$; da cui, per commutatività del diagramma, $\psi(\frac{au}{ut}) = \phi_{\overline{S}}(au)\phi_{\overline{S}}(ut)^{-1} = \frac{au}{ut} = \frac{a}{t}$.

□

Capitolo 6

Moduli Noetheriani e Artiniani

Lo studio di anelli Noetheriani e Artiniani ci permetterà di dimostrare degli utili risultati sulla decomposizione di ideali. Purtroppo non è stato possibile approfondire più di tanto questi concetti durante il corso, quindi alcuni risultati verranno solo enunciati senza essere dimostrati, o presentati come esercizio. Per il medesimo motivo, mi è capitato spesso di dover risolvere esercizi ricorrendo a risultati che non sono stati citati. Li aggiungerò poichè ritengo possano dare maggiore profondità a questa sezione, con la speranza che prima o poi ne compaiano anche delle dimostrazioni. Ad ogni modo, per venire incontro ai più tirchi di intelletto, mi preoccuperò di segnalarli, cosicchè possiate non studiare troppo[1].

Definizione 6.0.1. *Un anello A si dice* ***noetheriano*** *se soddisfa la ACC rispetto alle catene di ideali ordinate per inclusione. Un modulo M su un anello A si dice noetheriano se soddisfa la ACC rispetto alle catene di sottomoduli ordinate per inclusione.*

Definizione 6.0.2. *Un anello A si dice* ***artiniano*** *se soddisfa la DCC rispetto alle catene di ideali ordinate per inclusione. Un modulo M su un anello A si dice artiniano se soddisfa la DCC rispetto alle catene di sottomoduli ordinate per inclusione.*

Esempio.
- $\mathbb{K}[x_1, \ldots, x_n]$ è noetheriano ma non artiniano;
- $\mathbb{Z}$ è noetheriano ma non artiniano;
- $\mathbb{K}$ è noetheriano e artiniano.

Da questo momenton in poi, come prennunciato, molti dei risultati verranno solo enunciati, a cominciare dall'importantissimo

Teorema 6.1 (della Base di Hilbert)**.** *Se A è un anello noetheriano $\Rightarrow A[x]$ è un anello noetheriano.*

[1] Capre, capre, capre!

Proposizione 6.0.1. *Sia A anello. Le seguenti sono equivalenti:*

1. *A è noetheriano;*
2. *ogni ideale di A è finitamente generato;*

Lo stesso vale per M modulo noetheriano – chiaramente considerando i suoi sottomoduli al posto degli ideali.

La noetherianità risulta fondamentale nella dimostrazione di questi risultati perchè, ad esempio, permette di applicare con estrema facilità Zorn in quanto garantisce l'esistenza di un maggiorante per ogni catena ascendente di ideali o sottomoduli.

Lemma 6.0.1. *Siano M, M_1, M_2-moduli su un anello A e sia la seguente una successione esatta corta:*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

Allora valgono le seguenti equivalenze:

- *M è noetheriano $\Leftrightarrow M_1, M_2$ sono noetheriani;*
- *M è artiniano $\Leftrightarrow M_1, M_2$ sono artiniani;*
- *A noetheriano e M modulo su A finitamente generato $\Leftrightarrow M$ noetheriano.*

Se dunque scegliamo in modo opportuno la successione esatta corta, possiamo dimostrare il seguente corollario.

Corollario 6.1.1. *Sia A anello e $I \subseteq A$ ideale. Allora*

$$A \text{ è noetheriano } \Leftrightarrow {}^{A}/_{I} \text{ è noetheriano}$$

Dimostrazione. Basta applicare il lemma alla successione esatta corta

$$0 \longrightarrow I \longrightarrow A \longrightarrow {}^{A}/_{I} \longrightarrow 0$$

□

Esercizio. Sia A anello noetheriano, $S \subseteq A$ sottoinsieme moltiplicativamente chiuso. É vero che $S^{-1}A$ è noetheriano?

Usiamo una delle definizioni equivalenti: facciamo vedere che ogni ideale di $S^{-1}A$ è finitamente generato.
Sia $J \subseteq S^{-1}A$ ideale $\Leftrightarrow J = S^{-1}I$, con $I \subseteq A$ ideale. I è sicuramente

finitamente generato perchè A è noetheriano $\Rightarrow I = (f_1, ..., f_n)$. Se $\phi_S : A \longrightarrow S^{-1}A \mid a \mapsto \frac{a}{1}$, allora

$$J = I^e = (\frac{f_1}{1}, ..., \frac{f_n}{1}) \Rightarrow J \text{ è finitamente generato.}$$

L'ultimo risultato che enunciamo, del quale non penso aggiungeremo alcuna dimostrazione, caratterizza i moduli artiniani.

Teorema 6.2 (Caratterizzazione Anelli Artiniani)**.** *Sia A un anello. Allora*

$$A \text{ è artiniano } \Leftrightarrow A \text{ è noetheriano di dimensione } 0$$

Non dimostreremo il Teorema, ma vedremo nel dettaglio la dimostrazione del fatto che un Anello Artiniano abbia dimensione 0.

Lemma 6.0.2 (Facoltativo)**.** *Sia A un anello artiniano. Allora ogni ideale primo è anche massimale.*

Dimostrazione. Sia $\mathfrak{p}$ un ideale primo di $A \Leftrightarrow A/\mathfrak{p}$ è integro. Vogliamo far vedere che $\mathfrak{p}$ è anche massimale, ovvero che il quoziente è un campo. $A/\mathfrak{p}$ è artiniano poichè lo è A[2], possiamo dunque considerare la catena $(\overline{a}) \supseteq (\overline{a}^2) \supseteq ...$, con $\overline{a} \neq 0$, e affermare che $\exists k \in \mathbb{N} \mid \overline{a}^k = \overline{a}^{k+1} \Leftrightarrow \overline{a}^k(1 - \overline{ab}) = 0$. Poichè $A/\mathfrak{p}$ è un dominio, si ha $\overline{ab} = 1$. □

Osservazione. Sia A anello artiniano. Per quanto detto fin'ora, tutti i suoi ideali primi sono massimali. Allora, in particolare, se (0) è primo, ovvero se A è un dominio, non ci sono altri ideali. Ma se gli unici ideali sono (0) è A, allora A è un campo.

Esercizio. Sia A anello artiniano, $S \subseteq A$ sottoinsieme moltiplicativamente chiuso. Chi è $S^{-1}A$?

Prima di darci risposta, soffermiamoci sul seguente risultato.

Proposizione 6.0.2. *Sia A anello artiniano. Allora $A = A^* \cup D(A) = A^* \cup N(A)$.*

Dimostrazione. Sia $a \notin A^*$. Sfruttiamo la DCC: $(a) \supseteq (a^2) \supseteq (a^3) \supseteq ... \Rightarrow \exists k \in \mathbb{N} \mid a^k = a^{k+j} \ \forall j \in \mathbb{N}$, quindi $a^k = \alpha a^{k+1} \Leftrightarrow a^k(1 - \alpha a) = 0$. Se $1 - \alpha a = 0 \Rightarrow ai \in A^*$, ma $a \notin A^*$, da cui $a \in D(A)$.
L'uguaglianza tra $D(A)$ e $N(A)$ segue dal fatto che gli anelli artiniani siano anello noetheriani di dimensione 1, quindi tutti gli ideali primi sono massimale $\Rightarrow J(A) = D(A) = N(A)$. □

[2]Se non ne siete convinti, vi suggerisco di scrivere una ben precisa successione esatta corta e sfruttare alcuni risultati già enunciati.

Torniamo ora all'esercizio: cosa possiamo dire su $S^{-1}A$, se A è artiniano? Cominciamo con un caso particolare: supponiamo che A sia locale e artiniano. Allora, poichè primo e massimale sono equivalenti, e vi è un solo massimale, abbiamo anche un solo ideale primo. Per quanto visto fino ad adesso, possiamo scrivere $A = A^* \cup \mathfrak{m}$, e ridurre l'esercizio alla discussione di due casi:

- $S \cap \mathfrak{m} = \emptyset$
- $S \cap \mathfrak{m} \neq \emptyset$

Nel primo caso, stiamo aggiungendo gli inversi di elementi che erano già invertibili, quindi $S \cap \mathfrak{m} = \emptyset \Rightarrow S^{-1}A = A$.
Dedichiamoci ora al caso in cui $S \cap \mathfrak{m} \neq \emptyset$. $S^{-1}A = \overline{S}^{-1}A$, dove $\overline{S}$ è il saturato di S. Allora abbiamo

$$\overline{S} = A - \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$$

A è locale ed artiniano, quindi possiede un solo ideale primo e massimale, che è proprio $\mathfrak{m}$. Per questo motivo $\overline{S} = A - \{0\}$ e $S^{-1}A$ deve essere un campo. Precisamente, poichè se A artiniano segue che $A = A^* \cup D(A)$, se S interseca $\mathfrak{m} \subseteq D(A)$, questo deve necessariamente essere del tutto equivalente a 0 in $S^{-1}A$.

Esercizio. Sia $A = \mathbb{Z} \times \mathbb{Z}/(12) \times \mathbb{Q}$. Poichè il quoziente per un primo è integro, i primi di questo anello sono della forma $(p, 1, 1), (1, p, 1), (1, 1, p)$, con (p) primo nell'opportuno fattore. Sia ora $S = A - P$. Chi è $S^{-1}A$?

Facciamo un esempio esplicito: sia $A - P = \{(a, \overline{b}, c) \mid \overline{b} \not\equiv 0 \ mod(3)\}$. Intuitivamente, $S^{-1}A \cong \mathbb{Z}_{(3)}$. per dimostrarlo, proviamo a scrivere gli elementi di $S^{-1}A$ in una forma che ci possa aiutare nei conti.

$$\frac{(\alpha, \beta, \gamma)}{(t, u, v)} = \frac{(0, \beta, 0)}{(1, u, 1)} \Leftrightarrow \exists s \in S \mid s(\alpha, \beta u, \gamma) - (0, \beta u, 0)$$

Poichè possiamo scegliere $s = (0, 1, 0)$, tale equivalenza è sempre verificata. A questo punto è immediato l'isomorfismo con $\mathbb{Z}_{(3)}$.

Concludiamo questa parte con un esercizio di difficoltà elevata. Non è fondamentale risolverlo subito, ma ragionarvi può aiutare ad assimilare i concetti visti fino ad adesso. In particolare, permette di mettere bene a fuoco tutta una serie di dettagli dimostrativi ai quali si tende a prestare poca attenzione.

Esercizio (Esercizio 3, Luglio 2011)**.** Siano A, B, C anelli e siano $f : A \longrightarrow C$, $g : B \longrightarrow C$ omomorfismi surgettivi. Dimostrare che se A e B sono noetheriani allora $A \times_C B = \{(a, b) \in A \times B \mid f(a) = g(b)\}$ è noetheriano.

6.1 Decomposizione Primaria

Vedremo ora, in maniera rigorosa, come e perchè sia possibile decomporre gli ideali in intersezione di ideali primari.

Esercizio. Sia Q un ideale P-primario, ovvero un ideale primario tale che $\sqrt{Q} = P$. Allora valgono le seguenti affermazioni:

- $x \in Q \Rightarrow (Q : x) = A$;
- $x \notin Q \Rightarrow (Q : x)$ è P-primario;
- $x \notin P \Rightarrow (Q : x) = Q$.

Esercizio. Siano Q_1, Q_2 ideali P-primari. Allora anche $Q_1 \cap Q_2$ è P-primario.

Vorremmo riuscire a dire qualcosa in più sulla struttura degli ideali di un anello, e capire in seguito sotto quali ipotesi possiamo darne una buona descrizione.

Definizione 6.1.1. *$I \subseteq A$ si dice **ideale decomponibile** se $\exists Q_1, \cdots, Q_n$ ideali P_i-primari tali che $I = \bigcap_{i=1}^{n} Q_i$. In particolare, si parla di decomposizione* minimale *se*

$$\forall i \neq j \quad Q_i \not\supseteq \bigcap_{j \neq i} Q_j \ \wedge \ P_i \neq P_j.$$

Teorema 6.3. *Supponiamo di disporre di $I = \bigcap_{j=1}^{n} Q_j$ decomposizione minimale di $I \subseteq A$ ideale, con $P_j = \sqrt{Q_j}$ $\forall j = 1, \cdots, n$. Allora*

$$\{P_j\}_{j=1,\cdots,n} = \{\text{ideali primi } \in \Sigma\}, \quad \Sigma = \{\sqrt{(I : a)} \mid a \in A\}.$$

Dimostrazione. Cominciamo osservando che se scegliamo $a \in \bigcap_{i \neq j} Q_i$ e non in Q_j, abbiamo

$$\sqrt{(I : a)} = \sqrt{\left(\bigcap_{i=1}^{n} (Q_i : a)\right)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : a)} = P_j,$$

abbiamo quindi mostrato il contenimento $\subseteq$. D'altra parte, se $\sqrt{(I : a)}$ è primo, allora è un primo che è uguale all'intersezione di alcuni primi tra i P_i, quindi coincide con uno di questi. □

I primi P_i sono detti *primi associati* di I; gli elementi minimali tra di essi sono detti *primi minimali*, mentre gli altri sono detti *primi immersi*.

Lemma 6.1.1. *Sia A un anello in cui (0) è decomponibile. Allora:*

1. *$D(A) = \bigcup P_i$, dove P_i sono i primi associati a (0);*
2. *$N(A) = \bigcap P_i$, dove P_i sono i primi minimali di (0),*

Dimostrazione. La seconda affermazione l'avevamo già vista all'inizio del corso; si tratta solo di osservare che $N(A)$, in quanto radicale di (0), può essere ottenuto intersecando i primi minimali piuttosto che tutti i primi che contengono (0).
Abbiamo anche già visto che $D(A) = \bigcup_{a\neq 0} \sqrt{Ann(a)}$, quindi:

$$D(A) = \bigcup_{a\neq 0} \sqrt{Ann(a)} = \bigcup_{a\neq 0} \sqrt{(0:a)} = \bigcup P_i,$$

con P_i primi associati all'ideale (0). □

Vediamo come si applicano questi risultati al caso di un anello di frazioni.

Lemma 6.1.2. *Sia A anello, Q un ideale P-primario e sia S sottoinsieme moltiplicativamente chiuso. Allora:*

1. *$S \cap P \neq \emptyset \Rightarrow S^{-1}Q = S^{-1}A$;*
2. *$S \cap P = \emptyset \Rightarrow S^{-1}Q$ è $S^{-1}P$-primario.*

Dimostrazione. Vediamo il primo punto: sia $s \in S \cap P \Rightarrow s^n \in Q$ per qualche $n \in \mathbb{N} \Rightarrow Q \cap S \neq \emptyset \Rightarrow S^{-1}Q = S^{-1}A$. Per quanto riguarda invece il secondo punto, osserviamo che $\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$. Rimane da dimostrare che $S^{-1}Q$ è un ideale primario.

$$\frac{ab}{st} \in S^{-1}Q \Leftrightarrow \frac{ab}{1} \in S^{-1}Q \Leftrightarrow ab \in (S^{-1}Q)^c \Leftrightarrow ab \in Q$$

Se, dunque, supponiamo che $\frac{a}{1} \notin \S^{-1}Q \Leftrightarrow a \notin Q \Rightarrow b^n \in Q \Leftrightarrow (\frac{b}{1})^n \in S^{-1}Q$, quindi $S^{-1}Q$ è primario. □

Ma allora, se $I = \bigcap_{i=1}^{n} Q_i$, in che modo possiamo esprimere $S^{-1}I$?

$$S^{-1}I = S^{-1}\left(\bigcap_{i=1}^{n} Q_i\right) = \bigcap_{i=1}^{n}(S^{-1}Q_i)$$

Poichè $S^{-1}Q_i = A$ se $Q_i \cap S \neq \emptyset$, possiamo supporre di sta intersecando solo i Q_i che non intersecano S, quindi tali che $P_i = \sqrt{Q_i}$ non interseca S. Ma allora

$$S^{-1}I = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_n$$

è una decomposizione minimale dell'ideale $S^{-1}I$. Inoltre, se la contraiamo otteniamo $Q_1 \cap \cdots \cap Q_n$.

Teorema 6.4 (Decomposizione Primaria)**.** *Sia A noetheriano e sia $I \subseteq A$ ideale. Allora $\exists Q_1, \cdots, Q_n$ ideali primari tali che $I = \bigcap_{i=1}^{n} Q_i$*

Dimostrazione. La dimostrazione si compone di due passi: nel primo dimostriamo che ogni ideale si scrive come intersezione finita di irriducibili; nel secondo facciamo vedere che ogni irriducibile è primario.
Consideriamo la famiglia Σ degli ideali di A che *non* sono intersezione finita di ideali irriducibili e supponiamo per assurdo che non sia vuota. Per noetherianità, le ipotesi del Lemma di Zorn sono soddisfatte $\Rightarrow \exists J$ elemento massimale. Sicuramente J non è irriducibile $\Rightarrow J = J_1 \cap J_2$, dove $J_1 \supsetneq J$ e $J_2 \supsetneq J$; allora, per massimalità, sia J_1 che J_2 si scrivono come intersezione finita di irriducibili, ma questo è assurdo.
Ora mostriamo che ogni irriducibile I è primario. Consideriamo $A \,/\, I$ e $ab = 0$ in $A \,/\, I$; supposto che $b \neq 0$, vorremmo mostrare che $\exists n \in \mathbb{N} \mid a^n \in I$. Cerchiamo di sfruttare la noetherianità: $b \in Ann(a) \subseteq Ann(a^2) \subseteq Ann(a^3) \subseteq \cdots \Rightarrow$ $\exists n \in \mathbb{N}$ tale che $Ann(a^n) = Ann(a^{n+1})$. Allora, poichè $(a^n) \cap (b) = (0) \Leftrightarrow 0 = ka^n = hb \Rightarrow hab = 0 = ka^{n+1} \Rightarrow k \in Ann(a^{n+1}) = Ann(a^n) \Rightarrow ka^n = 0$. Poiché $b \neq 0$ in $A \,/\, I$ e (0) è irriducibile, $(a^n) = (0)$.
Precisiamo che (0) è irriducibile poiché $\pi : A \twoheadrightarrow A \,/\, I$ è surgettiva e tale che $Ker\pi \supseteq I$, quindi $I = I^{ec}$. Con queste ipotesi, se supponessimo $(0) = \pi(I)$ riducibile giungeremo ad assurdo poichè riusciremmo a ridurre I[3]. □

Esercizio (Esercizio 3.2, Febbraio 2016)**.** Dire se la seguente affermazione è vera e in tal caso dimostrarla; altrimenti fornire un controesempio.
Sia $(A, \mathfrak{m})$ anello noetheriano locale con ideale massimale $\mathfrak{m}$, e sia $\mathfrak{q}$ ideale $\mathfrak{m}$-primario. Allora $A \,/\, \mathfrak{q}$ è artiniano.

Segue un esercizio di un vecchio compito d'esame che richiede l'utilizzo di varie nozioni su decomposizione primaria e anelli di frazioni. La soluzione dell'esercizio è reperibile online, ma consiglio al lettore di risolvere i quesiti in autonomia e di esercitarsi a scriverne per bene la soluzione: è un efficiente strumento per valutare il grado di familiarità acquisito con questo argomento.

Esercizio (Esercizio 3, Febbraio 2013)**.** Sia A un anello e sia $D(A)$ l'insieme dei divisori di 0 di A. Sia $S = A - D(A)$ e sia $Q(A) = S^{-1}A$. Dimostrare che:

[3]Per convincersene è sufficiente il teorema di corrispondenza tra ideali di A che contengono I e ideali di $A \,/\, I$.

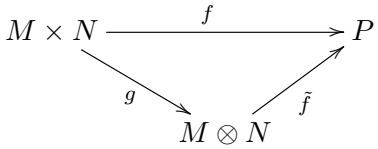
1. S è il più grande sottoinsieme moltiplicativamente chiuso tale che $\phi_s : A \longrightarrow S^{-1}A$ è iniettiva.
2. Se A è tale che $\forall a \notin A^* \Rightarrow a \in D(A)$, allora ϕ_S è bigettiva.
3. Se $A = B \,/\, \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n$ con B dominio e $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ ogni volta che $i \neq j$, allora $Q(A) = \oplus_{i=1}^{n} Q(B \,/\, \mathfrak{p}_i)$.
4. Sia $A = \mathbb{C}[x, y] \,/\, (x, y)$. Descrivere $Q(A)$.

Capitolo 7

Prodotto Tensore

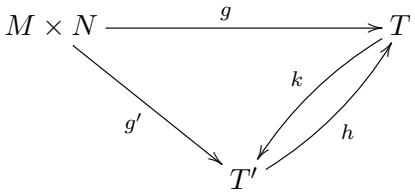
Siano dati M, N, P-moduli sull'anello A, e sia $f : M \times N \longrightarrow P$ una mappa A bilineare. Per mappa A bilineare, come al solito, si intende una applicazione f che sia A lineare in entrambe le sue componenti. In questa sezione cercheremo di generalizzare il concetto di bilinearità studiando la fattorizzazione di una mappa dotata di tale proprietà. Essenzialmente, dimostreremo che esiste un unico modulo T ed una sola mappa bilineare $g : M \times N \longrightarrow T$ tale che *ogni* mappa bilineare da $M \times N$ ad un qualsiasi A-modulo P fattorizza per g.
Un tale modulo T verrà chiamato **prodotto tensore** di M e N e indicato con $M \otimes_A N$.

Proposizione 7.0.1. *Siano M, N due A-moduli. Allora esiste una coppia (T, g), con T un A-modulo e $g : M \times N \to T$ bilineare, tale che ogni mappa A bilineare da $M \times N$ ad un modulo arbitrario P fattorizza per T. In simboli, $\forall f : M \times N \longrightarrow P$ bilineare $\exists \tilde{f} : M \otimes N \longrightarrow P$ tale che $\tilde{f} \circ g = f$.*



Inoltre, una coppia di oggetti con una tale proprietà è unica.

Dimostrazione. Dimostriamo l'unicità. Supponiamo che esistano (T, g) e (T', g') che verificano la proprietà richiesta. Allora esistono h e k che fanno commutare il seguente diagramma:



ovvero $h \circ g' = g$ e $k \circ g = g'$, da cui $h \circ k \circ g = g,\ k \circ h \circ g' = g' \Rightarrow h \circ k$ e $k \circ h$ sono isomorfismi.
Per quanto riguarda l'esistenza, collochiamoci per prima cosa nel modulo libero$A^{(M\times N)}$. Vorremmo definire una mappa g bilineare da $M \times N$ a qualche quoziente di $A^{(M\times N)}$. Poichè sappiamo bene quali proprietà richiedere alla mappa, consideriamo il sottomodulo D di $A^{(M\times N)}$ generato da tutti gli elementi del tipo:

- $(x + x', y) - (x, y) - (x', y)$
- $(x, y + y') - (x, y) - (x, y')$
- $(ax, y) - a(x, y)$
- $(x, ay) - a(x, y)$

Sia ora $T = A^{(M\times N)} \,/\, D$, e per ogni elemento $(x, y) \in M \times N$ denotiamo con $x \otimes y$ la sua immagine in T tramite g. Poichè $A^{(M\times N)}$ è generato dalle coppie della forma (x, y), T è generato dalle loro immagini, ovvero da elementi della forma $x \otimes y$. Per come sono stati definiti, si ha:

- $(x + x') \otimes y = x \otimes y + x' \otimes y$
- $x \otimes (y + y') = x \otimes y + x \otimes y'$
- $(ax) \otimes y = x \otimes (ay) = a(x \otimes y)$

In altre parole, la mappa $g : M \times N \longrightarrow T$ tale che $g(x, y) = x \otimes y$ è bilineare. A questo punto possiamo definire $\tilde{f}(x \otimes y) = f(x, y)$, così da avere commutatività; e siamo sicuri che sia ben definita perchè f applicata ad elementi di D è nulla per bilinearità. □

Seguono adesso alcune proprietà basilari del prodotto tensore.

1. $m \otimes_A 0 = 0 \otimes_A n = 0\ \forall m \in M, \forall n \in N$;
2. $M \otimes_A N =< \{m \otimes_A n \mid m \in M; n \in N\} >= M \otimes_A N$, e tali tensori sono detti elementari;
3. se $\{m_i\}_{i\in I}$ generano M e $\{n_i\}_{i\in J}$ generano N, allora $\{m_i \otimes_A n_j\}$ generano $M \otimes_A N$.

Esempio. Chi è $\mathbb{Z} \,/\, (5) \otimes_{\mathbb{Z}} \mathbb{Z} \,/\, (7)$? Osserviamo che $m \otimes 5n = 5(m \otimes n) = 5m \otimes n = 0 \otimes n = 0$, e analogamente $7m \otimes n = 7(m \otimes n) = m \otimes 7n = m \otimes 0 = 0$. La proprietà determinante, però, è che 5 è invertibile modulo 7 e viceversa, quindi possiamo effettuare il seguente passaggio: $(1m) \otimes n = (7 \cdot 3m) \otimes n = 3m \otimes 7n = 3m \otimes 0 = 0$.

Proposizione 7.0.2. *Se $m, n \in \mathbb{Z}$ sono coprimi, allora $\mathbb{Z} \,/\, (n) \otimes_{\mathbb{Z}} \mathbb{Z} \,/\, (m) = \{0\}$.*

Dimostrazione. Se m e n sono relativamente primi, allora $n \equiv 1\ mod(m)$ e viceversa. Sia n' l'inverso d n modulo m; allora $nn' \equiv 1\ mod(m)$. Possiamo dunque scrivere $x \otimes y = (nn')x \otimes y = n'x \otimes ny = n'x \otimes 0 = 0$, da cui la tesi. □

Esercizio. Descrivere $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.
Consideriamo l'applicazione $\mathbb{Z}$ bilineare $b : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} \mid (p, q) \mapsto pq$. Passando al tensore, abbiamo $\beta : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q} \mid (p \otimes q) \mapsto pq$. Osserviamo che $p \otimes q = x \otimes \frac{a}{b} = \frac{xb}{b} \otimes \frac{a}{b} = \frac{x}{b} \otimes a = \frac{xa}{b} \otimes 1$, quindi $\mathbb{Q} \otimes \mathbb{Q}$ è generato da tensori elementari del tipo $x \otimes 1$. $\beta(x \otimes 1) = b(x, 1) = x$, quindi sicuramente β è surgettiva; d'altra parte $\beta(x \otimes 1) = 0 \Leftrightarrow x = 0$, quindi è anche iniettiva.

Proposizione 7.0.3. *Siano M, N, P degli A-moduli. Allora esistono uniche delle mappe di isomorfismo tra i seguenti oggetti:*

1. $M \otimes N \longrightarrow N \otimes M$ *tale che* $x \otimes y \mapsto y \otimes x$
2. $(M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P) \longrightarrow M \otimes N \otimes P$ *tale che* $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$
3. $(M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$ *tale che* $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
4. $A \otimes M \longrightarrow M$ *tale che* $a \otimes x \mapsto ax$

Dimostrazione. Tutte le proposizioni si dimostrano nella stessa maniera, motivo per cui ne vedremo nello specifico solo alcune.

1. Consideriamo le seguenti mappe:

$$\begin{aligned} f : M \times N &\longrightarrow N \otimes_A N & \qquad g : N \times M &\longrightarrow M \otimes_A N \\ (m, n) &\mapsto n \otimes_A m & \qquad (n, m) &\mapsto m \otimes_A n \end{aligned}$$

   Entrambe passano al prodotto tensore, in quanto A bilineari, dunque abbiamo

$$\begin{aligned} \phi : M \otimes_A N &\longrightarrow N \otimes_A N & \qquad \psi : N \otimes_A M &\longrightarrow M \otimes_A N \\ m \otimes_A n &\mapsto n \otimes_A m & \qquad n \otimes_A m &\mapsto m \otimes_A n \end{aligned}$$

   Verifichiamo ora che $\psi \circ \phi = \mathrm{id}_{M \otimes_A B}$ e $\phi \circ \psi = \mathrm{id}_{N \otimes_A M}$.

$$\phi(\psi(n \otimes m) = \phi(m \otimes n) = n \otimes m$$

$$\psi(\phi(m \otimes n)) = \psi(n \otimes m) = m \otimes n$$

4. Sia $f : A \times M \longrightarrow M \mid (a, m) \mapsto am$ omomorfismo di A-moduli. f è chiaramente A bilineare, quindi induce una mappa $\tilde{f} : A \otimes M \longrightarrow M$. $\tilde{f} \circ g = f$, quindi $\tilde{f}$ è surgettiva; mostriamo che è anche iniettiva.

$$\tilde{f}(a \otimes m) = \tilde{f}(1 \otimes am) = \tilde{f}(1 \otimes \tilde{m}) = 1\tilde{m}$$

$$f(1 \otimes \tilde{m}) = 0 \Leftrightarrow \tilde{m} = 0$$

   dunque $\tilde{f}$ è un isomorfismo di A-moduli.

□

Corollario 7.0.1. *Sia A anello. Allora $A^n \otimes_A A^m = A^{nm}$.*

Dimostrazione.

$$A^n \otimes_A A^m = (\bigoplus_{j=1}^{n} A) \otimes_A (\bigoplus_{j=1}^{m} A) = \bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m}(A \otimes_A A) = \bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m} A = A^{nm}$$

□

Proposizione 7.0.4. *Siano M, N, P-moduli su A. Allora*

$$Hom_A(M \otimes_A N, P) \cong Hom_A(M, Hom(N, P)).$$

Dimostrazione. Esplicitiamo un isomorfismo:

$$\begin{aligned} \Psi : Hom_A(M \otimes_A N, P) &\longrightarrow Hom_A(M, Hom(N, P)) \\ g &\longmapsto \Psi(g) \end{aligned}$$

dove

$$\begin{aligned} g : M \otimes_A N &\longrightarrow P \\ m \otimes n &\mapsto g(m \otimes n) \end{aligned} \qquad \begin{aligned} \Psi(g) : M &\longrightarrow Hom(N, P) \\ m &\mapsto g_m \end{aligned}$$

e, infine,

$$\begin{aligned} g_m : N &\longrightarrow P \\ n &\longmapsto g(m \otimes n) \end{aligned}$$

Ψ è surgettiva perchè se $H \in Hom(M, Hom(N, P))$, allora $H(m, n) := H(m)(n)$ è bilineare, quindi passa al prodotto tensore come $\tilde{H}$, e chiaramente $\Psi(\tilde{H}) = H$.
Ψ è anche iniettiva perchè $\Psi(g) \equiv 0 \Leftrightarrow \ \forall m \in M g_m \equiv 0 \Leftrightarrow \ \forall m \in M, \forall n \in N \ g(m \otimes n) = 0$, da cui $g \equiv 0$. □

Osservazione. Osserviamo che l'isomorfismo appena dimostrato di dice che $Hom(N, \_)$ è l'aggiunto del funtore $\cdot \otimes_A N$ rispetto al funtore $Hom(\_, P)$.

Esercizio. Sia A un dominio e siano M, N due moduli su A. É vero che $T(M \otimes_A N) \cong T(M) \otimes_A T(N)$?

No, è falso. Scegliamo $A = \mathbb{Z}$ e consideriamo i moduli $\mathbb{Z}$ e $\mathbb{Z}/(6)$. Osserviamo che

$$T(\mathbb{Z}\Big/(6) \otimes_{\mathbb{Z}} \mathbb{Z}) = T(\mathbb{Z}\Big/(6)) = \mathbb{Z}\Big/(6)$$

$$T(\mathbb{Z}\Big/(6)) \otimes_{\mathbb{Z}} T(\mathbb{Z}) = T(\mathbb{Z}\Big/(6)) \otimes_{\mathbb{Z}} 0 = 0$$

Proposizione 7.0.5. *Siano $I, J \subseteq A$ ideali di un anello A. Allora*

$$A/I \otimes_A A/J \cong A/I + J$$

Dimostrazione. Per arrivare all'isomorfismo, sfruttiamo la seguente mappa

$$\begin{aligned} \psi : A/I \times A/J &\longrightarrow A/I + J \\ (a + I, b + J) &\longmapsto ab + I + J \end{aligned}$$

Si tratta di un'applicazione bilineare, quindi passa al tensore come

$$\begin{aligned} \Psi : A/I \otimes_A A/J &\longrightarrow A/I + J \\ (a + I) \otimes_A (b + J) &\longmapsto \psi(a + I, b + J) \end{aligned}$$

Ψ è l'isomorfismo desiderato. La surgettività segue dal fatto che ψ sia surgettiva, l'iniettività invece segue dalla seguente osservazione:

$$\psi(a + I, b + J) = 0 \Leftrightarrow ab \in I + J \Leftrightarrow ab = i + j,\ i \in I,\ j \in J.$$

Allora

$$(a + I) \otimes (b + I) = (1 + I) \otimes (ab + J) = (1 + I) \otimes (i + j + J) =$$

$$= (1 + I) \otimes (i + J) = (i + I) \otimes (1 + J) = (0 + I) \otimes (1 + J) = 0$$

quindi la mappa è anche iniettiva. □

7.1 Estensione e Restrizione di Scalari

In questa breve sezione mostreremo come, attraverso il prodotto tensore, sia possibile modificare la struttura di un modulo, estendendo o restringendo gli scalari rispetto ai quali è ben definita la moltiplicazione.
Consideriamo A e B anelli tali che $\exists f : A \longrightarrow M$ omomorfismo di anelli, quindi tale che $f(1_A) = 1_B$. Siano poi N un B-modulo e M un A-modulo.

- Si parla di **restrizione di scalari** quando si dota N di una struttura di A modulo definendo $\forall a \in A,\ \forall n \in N\ an = f(a)n$.

– Si parla, invece, di **estensione di scalari** quando si passa da M modulo su A al modulo M_B su B, definito come $M_B = B \otimes_A M$. Osserviamo che il prodotto tensore ha senso perchè B può essere visto come modulo su A definendo $\forall a \in A,\ \forall b \in B\ ab = f(a)b$, e che la struttura di B modulo è data dalla seguente definizione: $\forall b \in B\ b(b' \otimes m) = bb' \otimes m$.

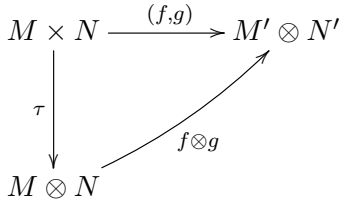
Esercizio (Esercizio 3.1, Febbraio 2016)**.** Dimostrare, se vera, la seguente affermazione, oppure trovare un controesempio.
Siano M modulo su $\mathbb{Z}$ e N modulo su $\mathbb{Q}$. Allora

$$Hom_{\mathbb{Z}}(M, N) \cong Hom_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q}, N) \text{ come moduli su } \mathbb{Z}$$

7.2 Moduli Piatti

Come nel caso dei Moduli Proiettivi, vorremmo discutere le proprietà del prodotto tensore vedendolo come funtore dalla categoria dei moduli su un anello A in sè. Come sappiamo, una categoria è data non solo da oggetti ma anche da morfismi tra di essi; per questo motivo, cominciamo discutendo il rapporto che vi è tra il prodotto tensore e gli omomorfismi di moduli.

Siano dati $f : M \longrightarrow M'$ e $g : n \longrightarrow N'$ omomorfismi di A-moduli; allora definiamo $f \otimes_A g : M \otimes_A N \longrightarrow M' \otimes_A N'$ come $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. Verifichiamo che si tratta di una buona definizione:



Effettivamente, la mappa $f \otimes g : (m \otimes n) \mapsto f(m) \otimes g(n)$ è quella che rende commutativo il diagramma, quindi la definizione è ben posta.
Se, inoltre, disponiamo di $f' : M' \longrightarrow M''$ e $g' : N' \longrightarrow N''$, definiamo la composizione come

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

Passiamo ora alla interpretazione funtoriale del prodotto tensore. Siano M, N, P, Q moduli su A, e sia la seguente una successione esatta:

$$M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

Il funtore $\cdot \otimes Q$ trasforma tale successione nella successione

$$M \otimes Q \xrightarrow{f \otimes \mathrm{id}_Q} N \otimes Q \xrightarrow{g \otimes \mathrm{id}_Q} P \otimes Q \longrightarrow 0$$

In generale, il funtore $\cdot \otimes Q$ è esatto a destra. Nel caso di alcuni moduli Q, viene preservata anche l'esattezza a sinistra, quindi il funtore è esatto. A tal proposito la seguente definizione.

Definizione 7.2.1. *Un modulo Q su un anello A si dice* ***modulo piatto*** *se il funtore $\cdot \otimes Q$ è esatto.*

Dimostriamo adesso che il funtore $\cdot \otimes Q$ è esatto a destra.

Proposizione 7.2.1. *Sia Q un modulo su A e sia*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una successione esatta. Allora anche

$$M' \otimes_A Q \xrightarrow{f\otimes_A \mathrm{id}_Q} M \otimes_A Q \xrightarrow{g\otimes_A \mathrm{id}_Q} M'' \otimes_A Q \longrightarrow 0$$

è una successione esatta.

Dimostrazione. Sfrutteremo l'esattezza a sinistra dei due funtori Hom. Poichè abbiamo a disposizione una successione esatta a destra, applichiamo il funtore Hom *controvariante*, $Hom(\_, Q)$, e osserviamo che:

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

è esatta *se e soltanto se*

$$0 \longrightarrow Hom_A(M'', Q) \longrightarrow Hom_A(M, Q) \longrightarrow Hom_A(M', Q)$$

è esatta. Ora, applicando il funtore Hom *covariante*, $Hom(Q, \_)$, abbiamo, come condizione equivalente, che anche la seguente successione è esatta:

$$0 \longrightarrow Hom_A(Q, Hom_A(M'', Q)) \longrightarrow$$

$$\longrightarrow Hom_A(Q, Hom_A(M, Q)) \longrightarrow Hom_A(Q, Hom_A(M', Q)).$$

Arrivati a questo punto ci serve un altro risultato che abbiamo da poco dimostrato:

$$Hom_A(M \otimes_A N, P) \cong Hom_A(M, Hom_A(N, P)).$$

Da questo segue l'esattezza della successione

$$0 \longrightarrow Hom_A(M'' \otimes_A Q, Q) \longrightarrow Hom_A(M \otimes_A Q, Q) \longrightarrow Hom_A(M' \otimes_A Q, Q)$$

che, per le proprietà del funtore $Hom(\_, Q)$ ci dice che la seguente successione è anch'essa esatta:

$$M \otimes_A Q \longrightarrow M \otimes_A Q \longrightarrow M' \otimes_A M'' \longrightarrow 0.$$

□

Esercizio (Esercizio 2, Luglio 2011)**.** Sia N modulo su A e $a \in N - D(A)$. Se N è piatto, allora $an \neq 0 \ \forall n \in N$

Le ipotesi ci suggeriscono di scrivere una successione esatta a sinistra e di tensorizzarla per N. Osserviamo dunque che

$$\begin{aligned} f_a : A &\longrightarrow A \\ b &\longmapsto ab \end{aligned}$$

è iniettiva poichè $a \notin D(A)$, quindi

$$0 \longrightarrow A \xrightarrow{f_a} A$$

è esatta a sinistra, da cui

$$0 \longrightarrow A \otimes_A N \xrightarrow{f_a \otimes_A \mathrm{id}_N} A \otimes_A N$$

è esatta a sinistra per piattezza di N. Ma questa ultima successione altro non è che

$$0 \longrightarrow N \xrightarrow{\cdot a} N$$

quindi $an \neq 0 \ \forall n \in N$.

Vista l'evidente analogia con la definzione dei Moduli Proiettivi, ci chiediamo quali altre proprietà già viste ritroviamo nei Moduli Piatti.

Esercizio. Siano N_1, N_2 due moduli su un anello A. Discutiamo la veridicità delle seguenti affermazioni:

1. N_1, N_2 piatti $\Leftrightarrow N_1 \oplus N_2$ piatto;
2. N_1, N_2 proiettivi $\Leftrightarrow N_1 \otimes_A N_2$ proiettivo;
3. N_1, N_2 piatti $\Leftrightarrow N_1 \otimes_A N_2$ piatto.

Dobbiamo verificare l'esattezza a sinistra.
In generale, se abbiamo T_1, T_2, Q_1, Q_2 A-moduli e

$$0 \longrightarrow T_1 \xrightarrow{t} T_2, \quad 0 \longrightarrow Q_1 \xrightarrow{q} Q_2$$

successioni esatte a sinistra, allora anche $0 \longrightarrow T_1 \oplus Q_1 \xrightarrow{(t,q)} T_1 \oplus Q_2$ è esatta a sinistra.
Sia ora $0 \longrightarrow M \xrightarrow{f} N$ esatta a sinistra.

$$0 \longrightarrow M \otimes_A (N_1 \oplus N_2) \xrightarrow{f \otimes_A id} N \otimes_A (N_1 \oplus N_2)$$

è esatta se e soltanto se $N_1 \oplus N_2$ è piatto. Poichè il prodotto tensore distribuisce rispetto alla somma diretta, si ha l'equivalenza del punto 1.

Un esercizio svolto da poco ci suggerisce la risposta al terzo quesito: $\mathbb{Z}/(5)\otimes_{\mathbb{Z}} \mathbb{Z}/(7) = 0$, dunque è sicuramente piatto, ma $\mathbb{Z}/(7)$ non è piatto poichè $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 7} \mathbb{Z}$ è esatta ma tensorizzando si perde l'iniettività. Il viceversa, invece, è vero per associatività del prodotto tensore.
Concludiamo con la seconda equivalenza. Quest'ultimo esempio ci dice che se il prodotto di tensore è proiettivo, non necessariamente lo sono i fattori – il controesempio è lo stesso. Invece è vero che il prodotto tensore di moduli proiettivi è proiettivo, in quanto i singoli fattori possono essere visti come addendi diretti di un moduli libero, e il prodotto tensore di moduli liberi è ancora libero, quindi proiettivo.

Esercizio. $\mathbb{Q}$ è piatto come modulo su $\mathbb{Z}$?

Diamo ora una nuova definizione di rango di un modulo.

Definizione 7.2.2. *Dato M modulo su A anello locale con ideale massimale $\mathfrak{m}$, definiamo il **rango** di M come $\mu(M) = dim_{\mathbb{K}}(M \otimes_A \mathbb{K})$, dove con $\mathbb{K}$ si intende $A/\mathfrak{m}$.*

Proposizione 7.2.2. *Sia $(A, \mathfrak{m})$ un anello locale e siano M, N moduli su A finitamente generati diversi da 0. Allora $M \otimes_A N \neq 0$.*

Dimostrazione. Faremo derivare questo risultato da uno più forte:

$$\mu(M \otimes N) = \mu(M) \cdot \mu(N).$$

Osserviamo infatti che

$$(M \otimes_A N) \otimes_A \mathbb{K} \cong M \otimes_A (N \otimes_A \mathbb{K}) \cong M \otimes_A (\mathbb{K} \otimes_A N) \cong$$

$$\cong M \otimes_A (\mathbb{K} \otimes_{\mathbb{K}} \mathbb{K}) \otimes_A N \cong M \otimes_A (\mathbb{K} \otimes_{\mathbb{K}} (\mathbb{K} \otimes_A N)) \cong (M \otimes_{\mathbb{K}} \mathbb{K}) \otimes_{\mathbb{K}} (\mathbb{K} \otimes_A N) \cong$$
$$\mathbb{K}^{\mu(M)} \otimes_{\mathbb{K}} \mathbb{K}^{\mu(N)} \cong \mathbb{K}^{\mu(N)\mu(M)}$$

□

Siamo ora pronti per dimostrare un risultato sui Moduli Proiettivi che avevamo lasciato in sospeso.

Proposizione 7.2.3. *Sia A anello locale, M modulo finitamente generato su A. Allora M è proiettivo $\Leftrightarrow$ M è libero.*

Dimostrazione. Sappiamo già che libero implica proiettivo; vediamo ora l'altra freccia.
M finitamente generato $\Rightarrow A^n \longrightarrow M \longrightarrow 0$ è esatta. Possiamo supporre $n = \mu(M) = dim_{\mathbb{K}}(M \otimes_A \mathbb{K}) = dim_{\mathbb{K}}(M/\mathfrak{m}M)$. Completiamo la successione e otteniamo

$$0 \longrightarrow Ker\phi \xrightarrow{i} A^n \xrightarrow{\phi} M \longrightarrow 0$$

M è proiettivo $\Leftrightarrow A^n = Ker\phi \oplus M$. Tensorizziamo per $\mathbb{K}$ e otteniamo:

$$A^n \otimes_A \mathbb{K} = (Ker\phi \oplus M) \otimes_A \mathbb{K} = {}^{Ker\phi}\big/_{\mathfrak{m}Ker\phi} \oplus {}^{M}\big/_{\mathfrak{m}M}$$

Ma è anche vero che $A^n \otimes_A A \,/\, \mathfrak{m} = \mathbb{K}^n$, che ha chiaramente dimensione n, da cui $H \,/\, \mathfrak{m}H \oplus M \,/\, \mathfrak{m}M$ ha dimensione n. Poichè, però, $M \,/\, \mathfrak{m}M$ ha dimensione n, segue $H \,/\, \mathfrak{m}H = 0 \Leftrightarrow H = \mathfrak{m}H$. Poichè l'anello è locale possiamo applicare la seconda formulazione del Lemma di Nakayama e concludere che $H = 0 \Rightarrow M = A^n$. □