Università di Pisa
Dipartimento di Matematica
Corso di Laurea Magistrale in Matematica

Appunti del Corso di Istituzioni di Algebra

A cura di
Rosario Mennuni

Titolare del Corso
Prof. Giovanni Gaiffi

Anno Accademico 2014/2015

Disclaimer

Questi appunti nascono dal corso di Istituzioni di Algebra tenuto dal professor Gaiffi[1] presso l'Università di Pisa durante il primo semestre dell'anno accademico 2014/2015. Sono inizialmente stati TEXati in diretta e corretti via via in collaborazione con Carlo Sircana (che ha poi abbandonato il progetto) e successivamente risistemati sotto la supervisione del professor Gaiffi. La responsabilità di sviste, errori, imprecisioni, carenze eccetera è mia, e l'indirizzo dove potete segnalarli è `mennuni@mail.dm.unipi.it`.

In alcuni punti mi sono preso la libertà di usare un linguaggio un po' più colloquiale del solito, di riportare alcuni trucchetti mnemonici che potrebbero essere ritenuti sconvenienti a seconda di come si interpretano le parole, e in generale di stemperare un attimino quell'aura di serietà austera (troppo?) comune in matematica. La responsabilità di questa — forse inappropriata — scelta è esclusivamente mia.

Mi sono permesso anche di aggiungere, in un paio di punti, qualche nota contenente informazioni "bonus" ad uso e consumo del lettore con interessi set-teoretici. È del tutto ragionevole che al resto dei lettori queste informazioni non interessino o, peggio, suonino spaventose/insensate/trascendentali: non vi preoccupate, sono aggiunte mie, non fanno parte del corso e — ai fini dell'esame — possono essere ignorate senza ritegno. La stessa cosa si applica anche a un paio di considerazioni categoriali fatte prima di dire cos'è una categoria e facenti uso di un concetto che nel corso non è stato definito.

Se state consultando questi appunti in formato .pdf vi potrebbe essere utile sapere che quando viene richiamato il nome di un risultato (che ne so, Teorema 6.30), cliccarci vi porta al risultato in questione, e anche indice, note a piè di pagina e riferimenti alla bibliografia sono muniti di hyperlinks, anche se non segnalati da orpelli grafici[2].

Un grazie a: Sabino Di Trani per le chiacchierate chiarificatrici, Camilla Moscardi per gli appunti delle lezioni in cui ero assente, Giorgio Mossa per il repository `git` su cui questo progetto è nato. Hanno scovato e pazientemente catalogato una numero di errori a 7 cifre (in binario): Agnese Barbensi, Gianluca Basso, Francesca Gregorio e Riccardo Morandin, che mi ha anche aiutato personalmente a correggerli.

L'ultima versione di questi appunti e il relativo sorgente sono disponibili presso `http://poisson.phc.unipi.it/~mennuni/`. Questa versione è stata compilata in data 17 marzo 2017. Per sapere cosa cambia rispetto alla versione precedente che avete scaricato tirate `diff` sui sorgenti. Il sorgente di questo documento è incorporato nel pdf: fate click destro sulle graffette.

Sorgente:  Logo Unipi: 

Rosario "Mufasa" Mennuni

[1] Con qualche lezione tenuta dal professor Maffei.

[2] È abbastanza comune circondarli con un quadrato rosso; ho evitato di proposito che questo succeda perché trovo che distragga l'occhio.

Indice

Parte I

Algebra Commutativa

Capitolo 1

Dipendenza Integrale

Per tutta la prima parte degli appunti, a meno di esplicita indicazione contraria, la parola "anello" sarà un diminutivo di "anello commutativo con unità". Di conseguenza anche "omomorfismo" significherà "omomorfismo di anelli con unità", il che significa che, perché $\varphi\colon A \to B$ sia un omomorfismo, fra le altre cose deve valere anche $\varphi(1_A) = 1_B$. Ad esempio la mappa $\varphi\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da $\varphi(n) = (n, 0)$ *non* soddisfa quanto sopra, e quindi *non* la considereremo un omomorfismo. Senza questa ipotesi saltano un po' di cose, ad esempio nell'esempio precedente $f^{-1}(\mathbb{Z} \times \{0\})$ non è un ideale primo, anche se contrazione di un primo. Nella seconda parte considereremo anche anelli non commutativi, ma comunque muniti di unità, e anche questa volta agli omomorfismi sarà richiesto di comportarsi di conseguenza.

Il testo principale di riferimento per questa prima parte è [2]. Altri testi consigliati sono [5], [12] e [13].

1.1 Estensioni Intere

Definizione 1.1. Siano $A \subseteq B$ anelli. Un elemento $x \in B$ si dice *intero* su A se x è radice di un polinomio *monico* $p \in A[x]$.

In sostanza la nozione è analoga a quella di "elemento algebrico" quando si parla di estensioni di campi, ed è immediato notare che in quel contesto le due nozioni coincidono. Per iniziare ad avere un'idea circa il significato della definizione iniziamo a notare che

Esempio 1.2. Nell'estensione $\mathbb{Z} \subseteq \mathbb{Q}$ gli x interi su $\mathbb{Z}$ sono tutti e soli gli elementi di $\mathbb{Z}$.

Dimostrazione. Sia $x = p/q$, con $(p, q) = 1$. Da una relazione di dipendenza

$$\left(\frac{p}{q}\right)^n + \sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i = 0$$

si ottiene, moltiplicando per q^n,

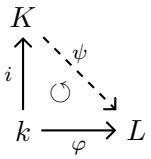
$$p^n = -\sum_{i=0}^{n-1} a_i p^i q^{n-i} = -q\left(\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right)$$

Di conseguenza, $q \mid p^n$; poiché siamo in un UFD e q e p sono coprimi q è invertibile. □

L'unica proprietà di $\mathbb{Z}$ che abbiamo usato è la fattorizzazione unica, e in effetti la stessa dimostrazione prova anche che

Proposizione 1.3. La stessa tesi vale rimpiazzando $\mathbb{Z}$ con un qualunque UFD e $\mathbb{Q}$ con il suo campo delle frazioni.

Dato che la definizione di elemento intero in estensioni di anelli generalizza quella di elemento algebrico in estensioni di campi può avere senso cercare di capire quali proprietà vengono "ereditate". Ad esempio se $k \subset K$ è un'estensione algebrica di campi ed $\varphi\colon k \to L = \bar{L}$ è un'immersione in un campo algebricamente chiuso, esiste ψ che fa commutare il diagramma[1]



Questo in genere viene dimostrato ad Algebra 1 per estensioni finite, ma si generalizza via Lemma di Zorn. In effetti la stessa cosa è vera quando $k \subset K$ è un'estensione intera di anelli, ma prima di dimostrarlo servirà un po' di lavoro. Iniziamo a vedere un po' di nozioni equivalenti a quella di elemento intero:

Teorema 1.4. Sia $A \subset B$ un'estensione di anelli e $x \in B$. Allora sono equivalenti:

1. x è intero su A
2. $A[x]$ è un A-modulo finitamente generato
3. $A[x] \subseteq C$, dove $C \subseteq B$ è un sottoanello che è un A-modulo finitamente generato
4. Esiste un $A[x]$-modulo *fedele* M, cioè tale che $\mathrm{Ann}(M) = 0$, che è finitamente generato come A-modulo.

[1] Il simbolo "↻" sottolinea il fatto che il diagramma commuti, ma è più un abbellimento che altro (nel senso che in alcuni diagrammi non ci sarà, ma questo non impedirà loro di commutare).

Dimostrazione.

(1 ⇒ 2) La relazione $p(x) = 0$ permette di limitare il grado dei polinomi, e ci bastano monomi di grado limitato per generare tutto $A[x]$.

(2 ⇒ 3) Basta prendere $C = A[x]$.

(3 ⇒ 4) Basta prendere $M = C$. Questo è fedele perché contiene 1, e quindi se $y \in \mathrm{Ann}(C)$ da $y \cdot 1 = 0$ si ha $y = 0$.

(4 ⇒ 1) Sia $\varphi = x\cdot \colon M \to M$ l'omomorfismo di A-moduli dato dalla moltiplicazione[2] per x. Dato che M è finitamente generato, per Cayley-Hamilton esistono degli $a_i \in A$ tali che $\varphi^n + \sum a_i \varphi^i = 0$. Questo vuol dire che la mappa $(x^n + \sum a_i x^i)\cdot$ è la mappa nulla, per cui $x^n + \sum a_i x^i \in \mathrm{Ann}(M) = \{0\}$ per fedeltà, e questo fornisce la dipendenza integrale cercata. □

Seguono subito un po' di analogie con le estensioni algebriche di campi:

Corollario 1.5. Siano $x_1, \ldots, x_n \in B$ interi su A. Allora $A[x_1, \ldots, x_n]$ è un A-modulo finitamente generato.

Che, nel caso dei campi, si legge "A-spazio vettoriale di dimensione finita". Senza chiedere l'interezza, ma solo l'algebricità (nel senso che permettiamo a p di non essere monico), questa cosa non è più vera: si pensi a $\mathbb{Z} \subseteq \mathbb{Z}[1/2]$.

Corollario 1.6. L'insieme $C \subseteq B$ degli elementi interi su A è un sottoanello di B.

Dimostrazione. Siano $x, y \in C$. Per vedere che $x + y \in C$ consideriamo $A[x + y] \subseteq A[x, y]$. Il secondo è finitamente generato, e basta porlo come C nel punto 3 del Teorema 1.4. Allo stesso modo, si mostra che $xy \in C$, mentre 1 è banalmente intero. □

Definizione 1.7. C come sopra si dice *chiusura integrale di A in B*. Se $C = A$ si dice che A è *integralmente chiuso* in B. Se $C = B$ si dice che B è *intero* su A.

"$-$ è intero su $-$" è una relazione transitiva:

Proposizione 1.8. Siano $A \subseteq B \subseteq C$ anelli e supponiamo che B sia intero su A e che C sia intero su B. Allora C è intero su A.

Dimostrazione. Sia $x \in C$, che in quanto intero su B soddisfa un'equazione del tipo $x^n + \sum b_i x^i = 0$, per opportuni $b_i \in B$. Se poniamo $B' = A[b_0, \ldots, b_{n-1}]$ abbiamo che x è banalmente intero su B', per cui $B'[x]$ è finitamente generato come B'-modulo, e dunque anche come A-modulo perché $B'[x] = A[b_0, \ldots, b_{n-1}][x]$ e i b_i sono interi su A. Basta allora invocare il terzo punto del Teorema 1.4. □

[2] Che ha senso perché M ha una struttura di $A[x]$-modulo.

Una conseguenza di questo fatto è che se $A \subseteq C \subseteq B$, dove C è la chiusura integrale di A in B, la chiusura integrale di C in B è sempre C o, in altre parole, la chiusura integrale è idempotente. Inoltre si comporta bene rispetto alle più popolari operazioni fra anelli:

Proposizione 1.9. Sia $A \subseteq B$ un'estensione intera, $\mathfrak{q}$ un ideale di B e $\mathfrak{p} = \mathfrak{q} \cap A$ la sua contrazione. Allora $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$.

Dimostrazione. Sia $x+\mathfrak{q} \in B/\mathfrak{q}$. Allora $x \in B$ è intero su A e dunque risolve un'equazione

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

Di conseguenza, riducendo modulo $\mathfrak{q}$ e usando il fatto che $\mathfrak{p} = A \cap \mathfrak{q}$,

$$(x+\mathfrak{q})^n + \sum_{i=0}^{n-1} (a_i + \mathfrak{p})(x+\mathfrak{q})^i = 0 \qquad \square$$

Proposizione 1.10. Siano $A \subseteq B$ anelli, C la chiusura integrale di A in B, S una parte moltiplicativa di A. Allora $S^{-1}C$ è la chiusura integrale di $S^{-1}A$ in $S^{-1}B$.

Dimostrazione. Sia $x/s \in S^{-1}C$, con $x^n + \sum a_i x^i = 0$, dove $a_i \in A$. Allora

$$\left(\frac{x}{s}\right)^n + \sum \frac{a_i}{s^{n-i}} \left(\frac{x}{s}\right)^i = 0$$

e quindi x/s è intero su $S^{-1}A$. Se viceversa $b/s \in S^{-1}B$ è intero su $S^{-1}A$ soddisfa un'equazione del tipo

$$\left(\frac{b}{s}\right)^n + \sum \frac{a_i}{s_i} \left(\frac{b}{s}\right)^i = 0$$

e basta porre $t = \prod s_i$ e moltiplicare per $(st)^n$ per avere che (bt) è intero su A e quindi appartiene a C. Ma allora $b/s = (bt)/(st) \in S^{-1}C$. $\square$

Esercizio 1.11. Siano $A \subseteq B$ domini e C la chiusura integrale di A in B. Dimostrare che la chiusura integrale di $A[t]$ in $B[t]$ è $C[t]$.

Prima di risolverlo facciamo la seguente

Osservazione 1.12. Nelle ipotesi dell'Esercizio, se $f, g \in B[t]$ sono monici e $fg \in C[t]$, allora $f, g \in C[t]$.

Dimostrazione dell'Osservazione. Indicando con $K(R)$ il campo dei quozienti di R la situazione è come in figura:

$$\begin{array}{ccccc} A & \hookrightarrow & C & \hookrightarrow & B \\ \downarrow & & \downarrow & & \downarrow \\ K(A) & \hookrightarrow & K(C) & \hookrightarrow & K(B) \hookrightarrow L \end{array}$$

dove L indica la chiusura algebrica di $K(B)$, in cui possiamo scrivere

$$f(t) = \prod(t-\alpha_i) \qquad g(t) = \prod(t-\beta_j) \qquad \prod(t-\alpha_i)\prod(t-\beta_j) = \underbrace{f(t)g(t)}_{\in C[t]}$$

Gli α_i e i β_j sono interi su C, e quindi su A per transitività. Dunque anche i coefficienti di f e g, in quanto somme e prodotti di interi su A, sono interi su A. Dato che, inoltre, questi coefficienti sono in B e che C è la chiusura integrale di A in B, abbiamo $f, g \in C[t]$. □

Soluzione dell'Esercizio. L'inclusione $C[t] \subseteq \overline{A[t]}$ è immediata: C è intero su A e a maggior ragione su[3] $A[t]$, e t è banalmente intero su $A[t]$ in quanto suo elemento; d'altronde somme e prodotti di interi sono interi. Se viceversa $f \in \overline{A[t]}$ prendiamo degli $h_i \in A[t]$ tali che $f^n + h_n + \sum h_i f^i = 0$. Riscriviamola come $f(f^{n-1} + \sum h_i f^{i-1}) = -h_n \in A[t] \subseteq C[t]$; se ora i due polinomi a sinistra sono monici l'Osservazione precedente conclude. Tuttavia ci si può sempre ricondurre al caso precedente sostituendo f con $f + t^r$, per r sufficientemente grande: infatti se $f + t^r \in C[t]$ chiaramente anche $f \in C[t]$. □

1.2 Ideali Primi ed Estensioni Intere

Finora aveva tutto un sapore di già visto. Ecco qualcosa di nuovo: supponiamo di avere un ideale primo $\mathfrak{p}$ di A e un'estensione intera B. Ci chiediamo se riusciamo a trovare[4] un primo $\mathfrak{q}$ tale che $\mathfrak{q}^c = \mathfrak{p}$:

$$\begin{array}{ccc} B & \supseteq & \mathfrak{q}? \\ \cup| & & \cup| \\ A & \supseteq & \mathfrak{p} \end{array}$$

Proposizione 1.13. Siano $A \subseteq B$ domini e B intero su A. Allora B è un campo se e solo se A lo è.

[3] Per il lettore (molto) scrupoloso: intendiamo che ogni elemento di C annulla un polinomio monico a coefficienti in $A[t]$. Ad essere (molto) fiscali abbiamo definito "S è intero su R" solo quando $R \subseteq S$, ma $A[t] \not\subseteq C$. Dato che $R \subseteq S$ serve per avere un "anello ambiente" dove "fare i conti", è sufficiente leggere C e $A[t]$ dentro $C[t]$.

[4] Come vedremo servirà, tra le altre cose, per l'estensione di omomorfismi di cui parlavamo prima.

Dimostrazione. Se B è un campo prendiamo $0 \neq x \in A$. Il suo inverso, in quanto elemento di B che è un'estensione intera, soddisfa un'equazione del tipo $(x^{-1})^m + \sum a_i (x^{-1})^i = 0$, con gli $a_i \in A$. Allora basta moltiplicare tutto per x^{m-1} per ottenere $x^{-1} = -\sum a_i x^{m-1-i}$.

Viceversa siano A un campo e $y \neq 0$ un elemento intero su A. Sia $y^n + \sum a_i y^i = 0$ un'equazione di grado minimo per y. Dato che A è un dominio deve essere $a_0 \neq 0$, perché altrimenti potremmo raccogliere y nell'equazione e ridurre il grado della relazione. Dunque a_0 è invertibile e possiamo scrivere[5]

$$y \left(a_0^{-1} \sum_{i=1}^{n} a_i y^{i-1} \right) = -1$$

che testimonia che y è invertibile. □

Notazione 1.14. Indichiamo con $\mathrm{Spec}(B)$ l'insieme degli ideali primi di B, e con $\mathrm{SpecMax}(B)$ l'insieme dei suoi ideali massimali.

Corollario 1.15. Sia $A \subseteq B$ un'estensione intera, $\mathfrak{q} \in \mathrm{Spec}(B)$ e $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}^c$. Allora $\mathfrak{q}$ è massimale se e solo se lo è $\mathfrak{p}$.

Dimostrazione. Per la Proposizione 1.9 $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$, ed è un dominio perché $\mathfrak{q}$ è primo. Dunque anche $A/\mathfrak{p}$ è un dominio perché incluso in un dominio, e basta usare la Proposizione precedente ricordandosi che $R/\mathfrak{a}$ è un campo se e solo se $\mathfrak{a}$ è massimale. □

Corollario 1.16. Se $A \subseteq B$ è un'estensione intera e $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$ sono ideali primi di B tali che $\mathfrak{q}_0^c = \mathfrak{q}_1^c = \mathfrak{p}$, allora $\mathfrak{q}_0 = \mathfrak{q}_1$.

Dimostrazione. Sia $S = A \setminus \mathfrak{p}$. Allora $A_\mathfrak{p} = S^{-1}A \subseteq S^{-1}B$ è intera e $S^{-1}\mathfrak{p} \subseteq S^{-1}A \subseteq S^{-1}B$. Notiamo che $S^{-1}\mathfrak{q}_0 \subseteq S^{-1}\mathfrak{q}_1$ si contraggono entrambi a $S^{-1}\mathfrak{p}$ e sono dunque massimali per il Corollario precedente, per cui coincidono. Per concludere basta ricordare che S^{-1} mette in bigezione gli ideali nell'anello di frazioni con gli ideali nell'anello che non intersecano S, e dunque $\mathfrak{q}_0 = \mathfrak{q}_1$. □

Teorema 1.17 (Lying Over)**.** Siano $A \subseteq B$ un'estensione intera e $\mathfrak{p} \in \mathrm{Spec}(A)$. Allora esiste $\mathfrak{q} \in \mathrm{Spec}(B)$ tale che $\mathfrak{q}^c = \mathfrak{p}$.

Dimostrazione. Poniamo di nuovo $S = A \setminus \mathfrak{p}$ e consideriamo il diagramma commutativo

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & B \\ \downarrow{\scriptstyle \frac{\cdot}{1}} & \circlearrowleft & \downarrow{\scriptstyle \frac{\cdot}{1}} \\ S^{-1}A & \xrightarrow[\ i\ ]{} & S^{-1}B \end{array}$$

[5] Qui chiaramente $a_n = 1$.

Prendiamo poi un qualunque $\mathfrak{m} \in \mathrm{SpecMax}(S^{-1}B)$ e seguiamo le sue contrazioni in A lungo i due lati del diagramma. Per il Corollario 1.15 $\mathfrak{m} \cap S^{-1}A$ è massimale, e quindi è $S^{-1}\mathfrak{p}$, che in A viene contratto a $\mathfrak{p}$. D'altra parte $\mathfrak{m} \cap B$ è un primo $\mathfrak{q} \in \mathrm{Spec}(B)$, che soddisfa la tesi perché per commutatività del diagramma $\mathfrak{q}^c = \mathfrak{p}$. □

Abbiamo appena fatto il passo base della dimostrazione del

Teorema 1.18 (Going Up)**.** Sia $A \subseteq B$ un'estensione intera. Sia

$$\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_n$$

una catena di ideali primi in A e supponiamo di avere una catena più corta $(m \leq n)$

$$\mathfrak{q}_0 \subseteq \ldots \subseteq \mathfrak{q}_m$$

di primi in B tali che $\mathfrak{q}_i^c = \mathfrak{p}_i$. Esistono allora ideali primi $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ che estendono la catena

$$\mathfrak{q}_0 \subseteq \ldots \subseteq \mathfrak{q}_m \subseteq \ldots \subseteq \mathfrak{q}_n$$

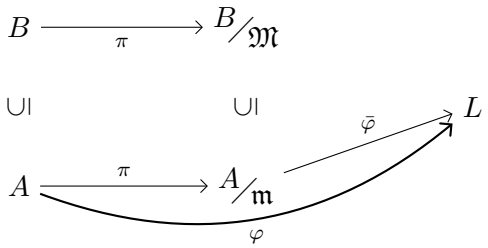
preservando la proprietà $\mathfrak{q}_i^c = \mathfrak{p}_i$.

Dimostrazione. Il caso $n = 0$, $m = -1$ è[6] il Lying Over, e per induzione possiamo ridurci al caso $n = 1$ e $m = 0$. Posti $\bar{A} = A/\mathfrak{p}_0$ e $\bar{B} = B/\mathfrak{q}_0$, l'estensione $\bar{B} \supseteq \bar{A}$ è intera, e per il Lying Over esiste $\overline{\mathfrak{q}}$ tale che $\overline{\mathfrak{q}}^c = \overline{\mathfrak{p}_1}$. Se $\pi\colon B \to B/\mathfrak{q}_0$ è la proiezione al quoziente basta porre $\mathfrak{q}_1 = \pi^{-1}(\overline{\mathfrak{q}})$ per ottenere la tesi. □

Come promesso dimostriamo ora che

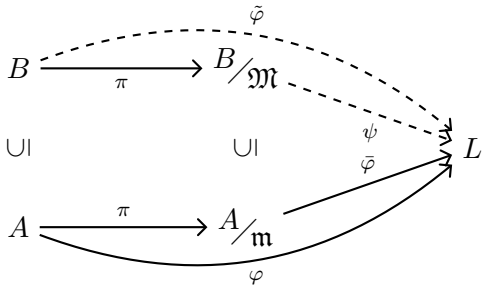
Teorema 1.19. Sia $A \subset B$ un'estensione intera e[7] $\varphi\colon A \to L \vDash \mathsf{ACF}$. Allora φ si estende ad un omomorfismo $\tilde{\varphi}\colon B \to L$.

Dimostrazione. Supponiamo dapprima che $\operatorname{Ker}\varphi = \mathfrak{m} \in \mathrm{SpecMax}(A)$. Per il Teorema del Lying Over esiste $\mathfrak{M} \in \mathrm{SpecMax}(B)$ tale che $\mathfrak{M}^c = \mathfrak{m}$. Fattorizzando φ otteniamo il diagramma

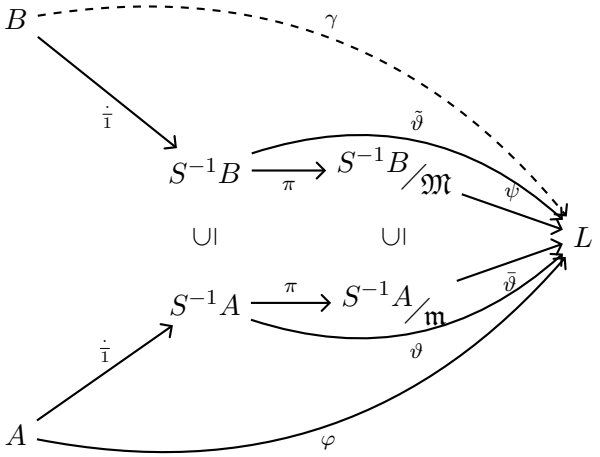


[6] Con "$m = -1$" intendiamo che non abbiamo ancora nessuna catena di B fra le mani.
[7] $L \vDash \mathsf{ACF}$ vuol dire che L è un campo algebricamente chiuso.

Dato che un'estensione intera di campi è algebrica esiste $\psi\colon B/\mathfrak{M} \to L$ che estende $\bar{\varphi}$, e basta porre $\tilde{\varphi} = \psi \circ \pi$.



Se invece $\mathfrak{p} = \operatorname{Ker}\varphi$ non è massimale è comunque primo perché $A/\mathfrak{p}$ si immerge in un campo ed è quindi un dominio. Localizziamo con $S = A \setminus \mathfrak{p}$ e troviamo $\vartheta\colon S^{-1}A \to L$ grazie alla proprietà universale degli anelli di frazioni. Ora $\operatorname{Ker}\vartheta$ è massimale e per quanto visto sopra possiamo estendere a $\tilde{\vartheta}$, e componendo come nel diagramma abbiamo l'estensione cercata γ.



□

1.3 Interi Quadratici

Studiamo la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, con d intero libero da quadrati. Osserviamo per prima cosa che se $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Z}$ è intero su $\mathbb{Z}$ soddisfa un polinomio del tipo $p(x) = x^n + \sum a_i x^i$; tuttavia α è algebrico su $\mathbb{Q}$ e dunque ammette un polinomio minimo $f(x) \in \mathbb{Q}[x]$ di grado[8] 2. Moltiplicando per i denominatori, otteniamo $\tilde{f}(x) \in \mathbb{Z}[x]$. Chiaramente $\tilde{f}(x) \mid p(x)$ in $\mathbb{Q}[x]$ per definizione di polinomio minimo, e per il Lemma

[8] Per l'Esempio 1.2 f non può avere grado 1.

di Gauss, $\tilde{f}(x) \mid p(x)$ in $\mathbb{Z}[x]$. Poiché $p(x)$ è monico, necessariamente anche $\tilde{f}(x)$ deve essere monico e dunque α soddisfa un polinomio di grado 2 monico a coefficienti interi.

Definizione 1.20. Sia $\alpha = x + y\sqrt{d}$ e indichiamo con σ l'automorfismo non identico del gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Allora $f(X) = (X - \alpha)(X - \sigma(\alpha)) = X^2 - (\alpha + \sigma(\alpha))X + \alpha\sigma(\alpha)$, e definiamo $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ rispettivamente *traccia* e *norma* di α, denotate con $T(\alpha)$ e $N(\alpha)$.

Proposizione 1.21. α è intero su $\mathbb{Z}$ se e solo se $T(\alpha), N(\alpha) \in \mathbb{Z}$.

Dimostrazione. Per la discussione precedente, se α è intero su $\mathbb{Z}$, allora $T(\alpha) \in \mathbb{Z}$ e $N(\alpha) \in \mathbb{Z}$. Viceversa, se $T(\alpha) \in \mathbb{Z}$ e $N(\alpha) \in \mathbb{Z}$, allora α è intero su $\mathbb{Z}$ perché annulla il polinomio $X^2 - T(\alpha)X + N(\alpha)$. □

Lemma 1.22. Sia $\alpha = x + y\sqrt{d}$ intero su $\mathbb{Z}$. Allora vale una e una sola delle seguenti:

- $x, y \in \mathbb{Z}$
- $x, y \notin \mathbb{Z}$

Dimostrazione. Notiamo che

$$\alpha + \bar{\alpha} = 2x \in \mathbb{Z} \qquad\qquad \alpha\bar{\alpha} = x^2 - dy^2 \in \mathbb{Z}$$

Supponiamo che sia $x \in \mathbb{Z}$. Allora $x^2 \in \mathbb{Z}$ e quindi $dy^2 \in \mathbb{Z}$. Se $y = s/t$, con $(s, t) = 1$ da $ds^2/t^2 \in \mathbb{Z}$, abbiamo $t^2 \mid ds^2$ e questo, visto che d è squarefree, implica $t = 1$ e quindi $y \in \mathbb{Z}$.

Se invece $x \notin \mathbb{Z}$, da $2x \in \mathbb{Z}$ otteniamo $x = s/2$ e $2 \nmid s$. Allora,

$$\frac{s^2}{4} - dy^2 = \frac{s^2 - 4dy^2}{4} \in \mathbb{Z}$$

quindi $4 \mid s^2 - 4dy^2$, e siccome $4 \nmid s^2$ deve essere $y^2 \notin \mathbb{Z}$, da cui la tesi. □

Notiamo ora che $T(2\alpha) = 2T(\alpha)$ e $N(2\alpha) = 4N(\alpha)$, quindi se α è intero su $\mathbb{Z}$ anche 2α lo è. Inoltre $2\alpha = 2x + 2y\sqrt{d}$, e $2x = T(\alpha) \in \mathbb{Z}$. Per il Lemma precedente anche $2y \in \mathbb{Z}$. Abbiamo così dimostrato che

Lemma 1.23. Sia α intero. Allora vale una e una sola delle seguenti:

- $x, y \in \mathbb{Z}$
- x, y sono della forma $\frac{2n+1}{2}$,

Supponiamo di avere $x = (2p+1)/2$ e $y = (2q+1)/2$. Abbiamo $T(\alpha) = 2p + 1$, mentre $N(\alpha) = \frac{1}{4}(4p^2 + 4p + 1) - \frac{d}{4}(4q^2 + 4q + 1) = p^2 + p - dq^2 - dq + (1 - d)/4 \in \mathbb{Z}$. Dunque α è intero se e solo se $1 - d \equiv 0 \pmod 4$. Dato che, a prescindere dalla classe di resto di d, se $x, y \in \mathbb{Z}$ si ha banalmente $T(\alpha), N(\alpha) \in \mathbb{Z}$, abbiamo dimostrato che

Teorema 1.24. Sia d squarefree.

- Se $d \equiv 2, 3 \pmod 4$ la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ è $\mathbb{Z}[\sqrt{d}]$.
- Se $d \equiv 1 \pmod 4$ la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ è $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Questi anelli sono ancora molto studiati; ad esempio se $d < 0$ è noto che ce ne sono solo 5 euclidei.

Esercizio 1.25. Trovare la chiusura integrale di $A = \mathbb{Z}[\sqrt{-3}, 1/2]$ in $\mathbb{Q}(\sqrt{-3})$.

Soluzione. Ponendo $S = \{2^n \mid n \in \mathbb{N}\}$ possiamo scrivere $A = S^{-1}\mathbb{Z}[\sqrt{-3}]$ e, denotando con B la chiusura integrale di $\mathbb{Z}[\sqrt{-3}]$ in $\mathbb{Q}(\sqrt{-3})$, abbiamo $\mathbb{Z}[\sqrt{-3}] \subset B \subset \mathbb{Q}(\sqrt{-3})$. Dato che la chiusura integrale si comporta bene con le frazioni[9] abbiamo

$$A = S^{-1}\mathbb{Z}[\sqrt{-3}] \subset S^{-1}B \subset \mathbb{Q}(\sqrt{-3})$$

Inoltre se un elemento è intero su $\mathbb{Z}[\sqrt{-3}]$ è intero anche su $\mathbb{Z}$ per transitività[10], e quindi B è la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-3})$, che abbiamo visto poco fa essere uguale a $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Ora bisogna capire chi è $S^{-1}B$, ma

$$S^{-1}B = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}, \frac{1}{2}\right] = \mathbb{Z}\left[\sqrt{-3}, \frac{1}{2}\right] = A$$

e ne concludiamo che A è integralmente chiuso in $\mathbb{Q}(\sqrt{-3})$. □

Esercizio 1.26. Dimostrare che se d è squarefree, $d < -7$ e $d \equiv 1 \pmod 8$, allora la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, cioè $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, *non* è un PID.

Soluzione. Mostriamo che addirittura non è un UFD mostrando che 2 è irriducibile ma non primo. Scriviamo

$$2 \;\Big|\; \frac{1-d}{4} = \left(\frac{1+\sqrt{d}}{2}\right)\left(\frac{1-\sqrt{d}}{2}\right)$$

Se 2 fosse primo dovrebbe dividere uno dei due fattori, quindi dovrebbe essere $2\alpha = \frac{1\pm\sqrt{d}}{2}$, che è assurdo, perché 2α dovrebbe essere della forma $m + n\sqrt{d}$, con $m, n \in \mathbb{Z}$. Per mostrare che 2 è irriducibile si procede come segue:

1. Si mostra che $N(\alpha\beta) = N(\alpha)N(\beta)$ (è un conto facile).
2. Si mostra che $N(2) = 4$ (è un conto ancora più facile).

[9] Vedi Proposizione 1.10.
[10] $\sqrt{-3}$ soddisfa una ben nota equazione quadratica.

3. Se $N(\alpha) = 1$, allora α è invertibile. Infatti se $1 = N(x + y\sqrt{d}) = x^2 - dy^2$, dato che $d < -7$, deve necessariamente essere $y = 0$, altrimenti $x^2 - dy^2 > 7y^2 > 1$. Ma allora deve essere $x = 1$ oppure $x = -1$.

4. Non esistono $\alpha \in A$ tali che $N(\alpha) = 2$. Se $2 = x^2 - dy^2$, deve essere $y \neq 0$ perché 2 non è un quadrato in $\mathbb{N}$ e $x \neq 0$ perché altrimenti avremmo $-d \mid 2$ in $\mathbb{N}$, contro $d < -7$. Si giunge così all'assurdo $2 = x^2 - dy^2 > x^2 + 7y^2 > 2$.

5. Dunque se $2 = \alpha\beta$ uno fra α e β deve essere invertibile. □

1.4 $\mathbb{K}$-algebre Finitamente Generate

Il Teorema 1.19 fornisce una dimostrazione alternativa di una forma debole del Nullstellensatz:

Teorema 1.27. Sia $\mathbb{K}$ un campo, $B = \mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra finitamente generata che è anche un campo. Allora B è un'estensione algebrica finita di $\mathbb{K}$.

L'idea della dimostrazione[11] è quella di applicare il risultato ottenuto per le estensioni intere dopo aver scomposto l'estensione $B \supseteq \mathbb{K}$ in una parte trascendente e una parte intera. Per fare questo si passa dal LNN:

Lemma 1.28 (di Normalizzazione di Noether)**.** Sia $\mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra finitamente generata[12]. Allora $\mathbb{K}[x_1, \ldots, x_n]$ è intero su $\mathbb{K}$, oppure esistono elementi $Y_1, \ldots, Y_r$ algebricamente indipendenti tali che $\mathbb{K}[x_1, \ldots, x_n]$ è intero su $\mathbb{K}[Y_1, \ldots, Y_r]$.

Dimostrazione. Se $x_1, \ldots, x_n$ sono algebricamente indipendenti basta porre $Y_i = x_i$. Supponiamo quindi che esista una relazione

$$0 = \sum_{(J)} a_{(J)} x_1^{J_1} \cdots x_n^{J_n} \tag{1.1}$$

dove $a_{(J)} \neq 0$ per ogni multi-indice (J). L'idea è ridurre induttivamente il numero di variabili per sostituzione: siano[13] $m_2, \ldots, m_n \in \mathbb{N} \setminus \{0\}$ e

[11] Che non vedremo, ma una che le somiglia molto è reperibile all'interno di [14]. Si veda anche l'Esercizio A.1.

[12] $x_1, \ldots, x_n$ sono generatori dell'algebra, non variabili. Per chiarezza indicheremo elementi algebricamente indipendenti in maiuscolo, quindi l'anello di polinomi sarà indicato con $\mathbb{K}[X_1, \ldots, X_n]$.

[13] Fisseremo questi m_i dopo, come gli ε in analisi.

prendiamo

$$\begin{aligned} y_2' &= x_2 - x_1^{m_2} \\ y_3' &= x_3 - x_1^{m_3} \\ \vdots \quad &\quad \vdots \quad \quad \vdots \\ y_n' &= x_n - x_1^{m_n} \end{aligned}$$

per poi sostituire nell'equazione (1.1) x_i con $y_i' + x_1^{m_i}$. Scrivendo $(m) = (1, m_2, \ldots, m_n)$ e denotando $(m)(J) = j_1 + m_2 j_2 + \ldots + m_n j_n$ otteniamo

$$\sum_{(J)} c_{(J)} x_1^{(m)(J)} + \underbrace{\varphi(x_1, y_2', \ldots, y_n')}_{\text{senza potenze pure in } x_1} = 0$$

Ci basta ora mostrare che x_1 è intero su $\mathbb{K}[y_2', \ldots, y_n']$ in maniera da poter procedere per induzione. Se riusciamo a scegliere (m) in modo che nella somma $\sum c_{(J)} x_1^{(m)(J)}$ non vi siano cancellazioni[14], allora a meno di dividere per il coefficiente di testa abbiamo la dipendenza integrale che cercavamo. Ma per non avere cancellazioni basta porre $k = 1 + \max_{(J)} J_i$ e $m = (1, k, k^2, \ldots, k^{n-1})$, e la tesi segue dall'unicità della scrittura in base k dei naturali. □

Osservazione 1.29. Dalla dimostrazione si ottiene anche che se $x_1, \ldots, x_n$ non sono algebricamente indipendenti allora $r < n$.

Sul LNN è basata la dimostrazione del Nullstellensatz cui si accennava prima, ed è collegato ad un mucchio di altre cose. Vediamolo un po' all'opera:

Definizione 1.30. Sia $\mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra finitamente generata. Una sua *base di trascendenza* è un insieme massimale di elementi $Y_1, \ldots, Y_r$ algebricamente indipendenti.

Esempio 1.31. Data una $\mathbb{K}$-algebra A finitamente generata, gli Y_i forniti dal LNN sono una base di trascendenza di A su $\mathbb{K}$. Ogni altro elemento x soddisfa infatti una relazione su $\mathbb{K}[Y_1, \ldots, Y_r]$ per interezza di A su $\mathbb{K}[Y_1, \ldots, Y_r]$ da cui la massimalità.

Potrebbe essere ragionevole pensare che due basi di trascendenza abbiano sempre la stessa cardinalità. Se così fosse, potremmo associare a una $\mathbb{K}$-algebra un numero che funga da "dimensione" prendendo la cardinalità di una base di trascendenza. Per $\mathbb{K}$-algebre sufficientemente belle[15] questo è possibile:

[14] Qui stiamo usando il fatto che φ non contribuisce al termine di grado massimo in x_1; questo segue, per come abbiamo fatto la sostituzione, dal fatto che non ha potenze pure in x_1.

[15] Per altre no: vedi Controesempio 1.35.

Teorema 1.32. Sia $\mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra che è anche un dominio e sia $Y_1, \ldots, Y_r$ una base di trascendenza. Allora se $W_1, \ldots, W_k$ sono algebricamente indipendenti si ha $k \leq r$.

Dimostrazione. Se ogni W_i coincide con un qualche Y_j la tesi è vera. Altrimenti sia WLOG $W_1 \notin \{Y_1, \ldots, Y_r\}$ e consideriamo $Y_1, \ldots, Y_r, W_1$. Per massimalità di $Y_1, \ldots, Y_r$ esiste una relazione

$$\sum_{(\rho)} a_{(\rho)} Y_1^{\rho_1} \cdots Y_r^{\rho_r} W_1^{\rho_{r+1}} = 0$$

dove $(\rho) = (\rho_1, \ldots, \rho_r, \rho_{r+1})$ e $a_{(\rho)} \neq 0$. Chiaramente sia W_1 che WLOG Y_1 devono comparire nella relazione con un esponente non nullo. Dunque Y_1 è algebrico sul campo delle frazioni $\mathbb{K}(Y_2, \ldots, Y_r, W_1)$, che esiste perché siamo su un dominio. Dato che $\mathbb{K}(x_1, \ldots, x_n)$ è algebrico su $\mathbb{K}(Y_1, \ldots, Y_r, W_1)$ (gli Y_i sono una base di trascendenza), l'estensione di campi $\mathbb{K}(x_1, \ldots, x_n) \supseteq \mathbb{K}(Y_2, \ldots, Y_r, W_1)$ è algebrica. Ne segue che W_2, in quanto elemento di $\mathbb{K}(x_1, \ldots, x_n)$, è algebrico su $\mathbb{K}(Y_2, \ldots, Y_r, W_1)$, e moltiplicando per i denominatori otteniamo una relazione di dipendenza algebrica

$$\sum_{(t)} b_{(t)} W_2^{t_1} Y_2^{t_2} \cdots Y_r^{t_r} W_1^{t_{r+1}} = 0$$

e concludiamo che $\mathbb{K}(x_1, \ldots, x_n)$ è algebrico su $\mathbb{K}(Y_3, \ldots, Y_r, W_1, W_2)$, come sopra. Procedendo induttivamente, se fosse $k > r$, arriveremmo a dire che $\mathbb{K}(x_1, \ldots, x_n) \supseteq \mathbb{K}(W_1, \ldots, W_r)$ è un'estensione algebrica e che W_{r+1} è algebrico su $W_1, \ldots, W_r$, contro le ipotesi. □

Osservazione 1.33. Il risultato è valido anche nel caso di $\mathbb{K}$-algebre non finitamente generate per basi di trascendenza infinite, a patto di modificare opportunamente la dimostrazione.

In base a quanto dimostrato è allora ben definito il grado di trascendenza:

Definizione 1.34. Sia $\mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra che è anche un dominio. Il *grado di trascendenza* $\operatorname{tr}_{\deg} \mathbb{K}[x_1, \ldots, x_n]$ è la cardinalità di una sua base di trascendenza.

Attenzione: senza l'ipotesi "dominio" il grado di trascendenza può smettere improvvisamente di funzionare:

Controesempio 1.35. In $\mathbb{K}[X] \times \mathbb{K}[Y, Z]$, sia $\{(X, 0)\}$ che $\{(0, Y), (0, Z)\}$ sono insiemi algebricamente indipendenti massimali, ma hanno cardinalità diversa. Infatti, ponendo $A = (X, 0)$, per qualunque scelta di $D = (p(X), q(Y, Z))$ l'insieme $\{A, D\}$ non è algebricamente indipendente, perché[16]

$$(p(A) - D)A = (p(X) - p(X), -q(Y, Z))(X, 0) = 0$$

[16]Stiamo valutando in (A, D) il polinomio $(p(\alpha) - \beta) \cdot \alpha$.

1.5 Domini Integralmente Chiusi

Siano A un dominio, K il suo campo dei quozienti e L un'estensione di K. Vogliamo collegare la nozione di elemento algebrico su K con quella di elemento intero su A. Se $x \in L$ è algebrico su K sia $f(t) = t^n + \sum a_i t^i$ il suo polinomio minimo, a coefficienti in K. Se tutti gli a_i sono in A allora x è ovviamente intero su A. È vero il viceversa? No:

Controesempio 1.36. Siano $A = \mathbb{Z}[\sqrt{5}]$ (e quindi $K = \mathbb{Q}(\sqrt{5})$) e $x = (1+\sqrt{5})/2 \in K$.

Il polinomio minimo di x su K è $t - x$, che *non* ha coefficienti in A, però x è comunque intero su A. Infatti

$$\left(t - \frac{1+\sqrt{5}}{2}\right)\left(t - \frac{1-\sqrt{5}}{2}\right) = t^2 - t - 1$$

Un'altra domanda che può saltarci in mente è se è vero un analogo del Going Up partendo "dall'ideale grande" invece che "da quello piccolo", che potremmo voler chiamare "Going Down". La risposta è anche stavolta "no":

Controesempio 1.37. Consideriamo la cubica[17] data da $f(x,y,z) = y^2 - x^3 - x^2$. L'omomorfismo

$$A = \frac{\mathbb{C}[x,y,z]}{(y^2 - x^3 - x^2)} \longrightarrow B = \mathbb{C}[t,z]$$

con $x \mapsto t^2 - 1$ e $y \mapsto t^3 - t$ (e $z \mapsto z$) rende B intero su A. Dati gli ideali $\mathfrak{q}_2 = (t+1, z-1)$, $\mathfrak{p}_2 = \mathfrak{q}_2 \cap A$, si ha che $\mathfrak{p}_1 = (y - zx) \subseteq \mathfrak{p}_2$, ma non esiste un ideale $\mathfrak{q}_1$ tale che $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

I dettagli del controesempio sono lasciati come esercizio[18].

Entrambe le cose sono però vere, come vedremo fra poco, in domini che soddisfano la seguente condizione:

Definizione 1.38. Un dominio si dice *integralmente chiuso* (tout-court) o *normale* se è integralmente chiuso nel suo campo dei quozienti.

Conosciamo già qualcuno di questi signori? Sì, ad esempio tutti gli UFD, come già visto nell'Esempio 1.2 e discussione seguente. Abbiamo anche già visto[19] che se $d \in \mathbb{Z}$ è squarefree allora $\mathbb{Z}[\sqrt{d}]$ è integralmente chiuso se e solo se $d \equiv 2 \pmod 4$ o $d \equiv 3 \pmod 4$. Ci sono anche domini integralmente chiusi che non sono UFD, e ne abbiamo anche già incontrati un po' nell'Esercizio 1.26. Mostriamo subito uno dei due risultati anticipati.

[17] Vista in $\mathbb{R}^3$ è tipo un foglio che si autointerseca.

[18] Di cui è presente una soluzione dettagliata in appendice. Vedi Esercizio A.2

[19] Teorema 1.24.

Proposizione 1.39. Sia A integralmente chiuso, K il suo campo dei quozienti[20], $K \subset L$ un'estensione di campi e $x \in L$. Allora x è intero su A se e solo se

1. x è algebrico/intero su K e
2. il polinomio minimo f_x di x su K è a coefficienti in A, cioè $f_x \in A[t]$

Dimostrazione. La freccia "$\Leftarrow$" è ovvia, come anche il punto 1 della freccia "$\Rightarrow$", per cui ci resta solo da mostrare che se x è intero su A vale il punto 2. Sia $f_x = t^n + \sum a_i t^i \in K[t]$ il polinomio minimo di x e sia M un'estensione normale di K che contiene x e tutte le radici di f_x (ad esempio la sua chiusura algebrica). Mostriamo che ogni altra radice y di $f(x)$ è intera su A. Come noto dalla Teoria di Galois esiste un automorfismo $\sigma \in \mathrm{Aut}(M/K)$ tale che $\sigma(x) = y$. Dato che x è intero su A prendiamo $g(t) = t^m + \sum b_i t^i \in A[t]$ tale che $g(x) = 0$. Allora

$$0 = \sigma(0) = \sigma(g(x)) = \sigma(x)^m + \sum b_i \sigma(x)^i = y^m + \sum b_i y^i$$

Dunque tutte le radici di f_x sono intere su A. Dato che i coefficienti a_i di f_x sono le funzioni simmetriche delle radici, che sono loro somme e prodotti, gli a_i sono tutti interi su A e dunque, per l'ipotesi di chiusura integrale, $a_i \in A$, che è la tesi. □

La chiusura integrale fa parte della lista delle proprietà locali:

Lemma 1.40. Sia A un dominio. Sono equivalenti:

1. A è integralmente chiuso.
2. Se $\mathfrak{p} \in \mathrm{Spec}(A)$ allora $A_\mathfrak{p}$ è integralmente chiuso.
3. Se $\mathfrak{m} \in \mathrm{SpecMax}(A)$ allora $A_\mathfrak{m}$ è integralmente chiuso.

Dimostrazione.

($1 \Rightarrow 2$) Consideriamo $A \subset A_\mathfrak{p} \subset K$. Sappiamo che $\overline{A}^K = A$, ma posto $S = A \setminus \mathfrak{p}$, usando la Proposizione 1.10 e il fatto che $S^{-1}K = K$,

$$\overline{A_\mathfrak{p}}^{S^{-1}K} = \overline{S^{-1}A}^{S^{-1}K} = S^{-1}\overline{A}^K = S^{-1}A = A_\mathfrak{p}$$

($2 \Rightarrow 3$) Ovvio.

($3 \Rightarrow 1$) Se $x \in K$ è intero su A in particolare è intero su $A_\mathfrak{m} \supset A$, quindi

$$x \in M = \bigcap_{\mathfrak{m} \in \mathrm{SpecMax}\, A} A_\mathfrak{m} \supseteq A$$

[20] Chiaramente stiamo supponendo tacitamente che A sia un dominio. Lo rifaremo.

Basta mostrare che $M \subset A$ per concludere. Se per assurdo ci fosse $x \in M \setminus A$ l'ideale $I = \{a \in A \mid ax \in A\}$ sarebbe proprio e quindi contenuto in un massimale $\mathfrak{m}$. Dato che $x \in M \subset A_{\mathfrak{m}}$ possiamo scrivere $x = y/s$ con $y \in A$ e $s \notin \mathfrak{m}$, e a maggior ragione $s \notin I$, contro $sx = y \in A$. □

Per dimostrare il Teorema del Going Down bisogna parlare di elementi interi su ideali:

Definizione 1.41. Sia $A \subset B$ e I un ideale di A. Un elemento $x \in B$ è *intero su* I se esiste $f(t) = t^n + \sum a_i t^i$ tale che $f(x) = 0$ e $\forall i\ a_i \in I$.

Lemma 1.42. Siano $I \subset A \subset B$ come sopra. Allora

$$\overline{I} \coloneqq \{x \in B \mid x \text{ è intero su } I\} = \sqrt[\overline{A}]{\overline{A}I}$$

dove $\overline{A}I$ è l'ideale generato da I in $\overline{A}$ e con $\sqrt[\overline{A}]{\ }$ intendiamo il radicale in $\overline{A}$.

Dimostrazione. L'inclusione "$\subseteq$" è ovvia: da $x^n = \sum a_i x^i \in \overline{A}I$ segue immediatamente $x \in \sqrt[\overline{A}]{\overline{A}I}$. Viceversa se $x \in \sqrt[\overline{A}]{\overline{A}I}$ possiamo scrivere $x^n = \sum a_i x_i \in \overline{A}I$ con gli $a_i \in I$ e gli $x_i \in \overline{A}$. Questo vuol dire che se definiamo l'A-modulo $M = A[x_1, \ldots, x_k]$, chiaramente finitamente generato, e l'omomorfismo di A-moduli $\varphi(u) = x^n u$ allora $\varphi(M) \subset IM$. Dunque per Hamilton-Cayley esistono dei $b_i \in I$ tali che $\varphi^z + \sum b_i \varphi^i = 0$, e perciò $x^{nz} + \sum b_i x^{ni} = 0$. □

È vero un analogo della Proposizione 1.39:

Proposizione 1.43. Sia A integralmente chiuso, K il suo campo dei quozienti, $K \subset L$ un'estensione di campi, $x \in L$ e I un ideale di A. Allora x è intero su I se e solo se

1. x è algebrico/intero su K e
2. il polinomio minimo f_x di x su K è della forma $t^n + \sum a_i t^i$, con gli $a_i \in \sqrt{I}$

Dimostrazione. Il verso "$\Rightarrow$" della dimostrazione è identico a quello della Proposizione 1.39 una volta osservato che, per il Lemma precedente, gli elementi di K interi su I sono $\sqrt{I}$, che è chiuso per somme e prodotti. Per il verso "$\Leftarrow$", da $x^n + \sum a_i x^i = 0$ si ha che x è intero su $\sqrt{I}$, ma per il Lemma precedente questo è la chiusura integrale di I. □

Richiamiamo il seguente risultato, che dovrebbe essere noto da Algebra 2[21]:

Lemma 1.44. Sia $\varphi\colon A \to B$ un omomorfismo di anelli e sia $\mathfrak{p}$ un primo di A. Allora $\mathfrak{p}$ è la contrazione di un ideale primo di B se e solo se $\mathfrak{p}^{ec} = \mathfrak{p}$.

[21] Comunque reperibile in [2] col nome di Proposizione 3.16.

Siamo finalmente pronti per dimostrare il

Teorema 1.45 (Going Down)**.** Siano $A \subset B$ domini con A integralmente chiuso e B intero su A. Sia

$$\mathfrak{p}_0 \supseteq \ldots \supseteq \mathfrak{p}_n$$

una catena di ideali primi in A e supponiamo di avere una catena più corta $(m \leq n)$

$$\mathfrak{q}_0 \supseteq \ldots \supseteq \mathfrak{q}_m$$

di primi in B tali che $\mathfrak{q}_i^c = \mathfrak{p}_i$. Esistono allora ideali primi $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ che estendono la catena

$$\mathfrak{q}_0 \supseteq \ldots \supseteq \mathfrak{q}_m \supseteq \ldots \supseteq \mathfrak{q}_n$$

preservando la proprietà $\mathfrak{q}_i^c = \mathfrak{p}_i$.

Dimostrazione. Come per il Going Up, a meno di induzione possiamo occuparci del caso $A \supset \mathfrak{p}_1 \supset \mathfrak{p}_2$ e $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Se nel Going Up si quozienta, qui si localizza: vogliamo mostrare che $\mathfrak{p}_2$ è la contrazione[22] di un primo $\mathfrak{p}$ di $B_{\mathfrak{q}_1}$, e per il Lemma appena richiamato basta mostrare che $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$.

$$\begin{array}{ccccc} A & \supset & \mathfrak{p}_1 & \supset & \mathfrak{p}_2 \\ \cap & & \cap & & \cap \\ B & \supset & \mathfrak{q}_1 & \supset & \mathfrak{q}_2 \\ \cap & & \cap & & \cap \\ B_{\mathfrak{q}_1} & \supset & \mathfrak{q}_1 B_{\mathfrak{q}_1} & \supset & \mathfrak{p} \end{array}$$

L'inclusione "$\supseteq$" è ovvia, per cui ci occupiamo direttamente della "$\subseteq$". Sia $x = y/s \in \mathfrak{p}_2 B_{\mathfrak{q}_1}$, con $y \in \mathfrak{p}_2 B$ e $s \in B \setminus \mathfrak{q}_1$. Dato che l'estensione $A \subseteq B$ è intera, per il Lemma 1.42 y è intero su $\mathfrak{p}_2$, per cui per la Proposizione 1.43 il suo polinomio minimo in[23] $K[t]$ è della forma $t^r + \sum u_i t^i$, con gli $u_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. Se ora $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$ possiamo scrivere $s = yx^{-1}$, dove $x^{-1} \in K$. Allora dividendo $y^r + \sum u_i y^i = 0$ per x^r otteniamo $s^r + \sum v_i s^i = 0$. C'è di più: $t^r + \sum v_i t^i$ è proprio il polinomio minimo di s, perché se ce ne fosse uno di grado $d < r$ ne otterremmo uno di grado minore anche per y moltiplicando $s^d + \sum \ldots$ per una potenza di x opportuna. Dato che s, come tutti gli elementi di B, è intero su A allora per la Proposizione 1.39 abbiamo $v_i \in A$. Però $v_i = u_i/x^{r-i}$, per cui $x^{r-i} v_i = u_i \in \mathfrak{p}_2$, e se per assurdo fosse $x \notin \mathfrak{p}_2$ allora tutti i v_i sarebbero in $\mathfrak{p}_2$ e da $s^r + \sum v_i s^i = 0$ avremmo $s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$, ma $\mathfrak{q}_1$ è primo e quindi abbiamo $s \in \mathfrak{q}_1$, contraddicendo il fatto che $s \notin \mathfrak{q}_1$. □

[22] Secondo la mappa di inclusione (per i domini S^{-1} è iniettiva).

[23] Stiamo ancora denotando con K il campo dei quozienti di A.

1.6 Risultati in Ambiti Non Commutativi

Ci occupiamo ora di due risultati che, per quanto possa sembrare strano a leggerne gli enunciati, seguono dal lavoro fatto in algebra commutativa. Durante il corso il prof. Frigerio ha tenuto un seminario sulle applicazioni di questi risultati in geometria, trascritto nell'Appendice B di questi appunti.

Teorema 1.46 (Lemma di Selberg)**.** Ogni sottogruppo finitamente generato Γ di $\mathrm{GL}(n, \mathbb{C})$ ha un sottogruppo normale, libero da torsione e di indice finito.

Teorema 1.47 (di Residuale Finitezza)**.** Ogni $G < \mathrm{GL}(n, \mathbb{C})$ finitamente generato è *residualmente finito*, ossia $\forall g \in G \setminus \{1\}$ esiste un omomorfismo φ_g da G a un gruppo finito tale che $\varphi_g(g) \neq 1$.

Faremo pesante uso del seguente risultato:

Teorema 1.48. Sia $B \supseteq A$ un dominio finitamente generato come A-algebra, e sia $b \in B \setminus \{0\}$. Allora esiste $a \in A \setminus \{0\}$ tale che ogni omomorfismo $\alpha \colon A \to L \vDash \mathsf{ACF}$ tale che $\alpha(a) \neq 0$ può essere esteso ad un omomorfismo $\beta \colon B \to L$ tale che $\beta(b) \neq 0$.

Dimostrazione. A meno di procedere per induzione sul numero di generatori possiamo assumere $B = A[x]$. Distinguiamo due casi:

1. x è algebrico sul campo delle frazioni $k(A)$
2. x non è algebrico su $k(A)$

Supponiamo prima che x non sia algebrico su $k(A)$. Possiamo scrivere, per opportuni $a_i \in A$ e $a_0 \neq 0$,

$$b = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = \sum_{i=0}^{n} a_{n-i} x^i$$

Mostriamo che $a = a_0$ soddisfa la tesi. Sia $\alpha \colon A \to L$ un omomorfismo tale che $\alpha(a) \neq 0$, e consideriamo il polinomio in $L[t]$

$$p(t) = \underbrace{\alpha(a_0)}_{\neq 0} t^n + \ldots + \alpha(a_n)$$

Dato che L è algebricamente chiuso è in particolare infinito, per cui esiste sicuramente $y \in L$ tale che $p(y) \neq 0$. Basta allora estendere l'omomorfismo con $x \mapsto y$ per avere la tesi[24].

[24] Dato che stiamo assumendo che x non sia algebrico su $k(A)$ è facile vedere che questa è una buona definizione.

Occupiamoci ora del primo caso. Abbiamo

$$b \in B = A[x] \subseteq k(A)[x] \subseteq k(B)$$

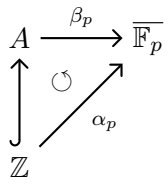
Dato che $b \in k(A)[x]$ e x è algebrico su $k(A)$, anche b lo è; a meno di eliminare i denominatori possiamo allora trovare una relazione $\sum_{i=0}^{n} d_i b^i = 0$, con i $d_i \in A$ e $d_n \neq 0$, e dato che B è un dominio possiamo anche supporre $d_0 \neq 0$, a meno di abbassare il grado della relazione. Moltiplicando per $b^{-n} \in k(B)$ otteniamo

$$d_0 b^{-n} + \ldots + d_n = 0 \tag{1.2}$$

Dato che x è algebrico su $k(A)$ soddisfa una relazione del tipo $\sum_{j=0}^{m} c_{m-j} x^j$, con i $c_j \in A$ e $c_0 \neq 0$. Poniamo $a = d_0 \cdot c_0 \in A$ e vediamo che anche in questo caso soddisfa la tesi. Se $\alpha\colon A \to L$ è tale che $\alpha(a) \neq 0$, per la proprietà universale degli anelli di frazioni può essere esteso a $\alpha'\colon S^{-1}A \to L$, dove $S = \{a^i \mid i \in \mathbb{N}\}$. Ora, in $S^{-1}A = A[a^{-1}]$, sono invertibili sia d_0 che c_0, e l'estensione $A[a^{-1}] \subseteq A[a^{-1}][b^{-1}]$ è intera perché possiamo invertire il coefficiente di testa nella (1.2). Applicando due volte il Teorema 1.19 possiamo dunque estendere α' prima ad $\alpha''\colon A[a^{-1}][b^{-1}] \to L$ e poi alla chiusura integrale di $A[a^{-1}]$ in $k(B)$, che battezziamo C, ottenendo $\alpha'''\colon C \to L$. Se ora mostriamo che $B \subseteq C$ e che $b^{-1} \in C$ per ottenere la tesi basta porre $\beta = \alpha'''_{\restriction B}$, perché se $b, b^{-1} \in C$, allora $\beta(bb^{-1}) = \beta(1) = 1$ e dunque $\beta(b) \neq 0$. Ma dato che b^{-1} è intero su $A[a^{-1}]$, che $B = A[x]$ e che x è intero su[25] $A[a^{-1}]$ l'inclusione $B \cup \{b^{-1}\} \subseteq C$ è ovvia per definizione di chiusura integrale. □

Teorema 1.49. Supponiamo di avere un sottoanello di $\mathbb{C}$ che sia una $\mathbb{Z}$-algebra finitamente generata $A = \mathbb{Z}[a_1, \ldots a_m] \subseteq \mathbb{C}$. Allora ogni sottogruppo di[26] $\mathrm{GL}(n, A)$ ha un sottogruppo normale di indice finito libero da torsione.

Dimostrazione. Dato che $A \subset \mathbb{C}$ e ogni sottoanello di un dominio è un dominio possiamo invocare il Teorema precedente con $\mathbb{Z}$ nelle vesti di A (del Teorema precedente), A (di questo Teorema) nelle vesti di B, e $b = 1$, ottenendo $a \in \mathbb{Z}$. Per ogni $p \in \mathbb{Z}$ primo, definiamo $\alpha_p\colon \mathbb{Z} \to \overline{\mathbb{F}_p}$ come la composizione della proiezione al quoziente su $\mathbb{F}_p$ con l'immersione nella sua chiusura algebrica. Poiché solo finiti primi dividono a abbiamo infinite mappe α_p tali che $\alpha_p(a) \neq 0$ e possiamo estendere ognuna di queste a rispettive $\beta_p\colon A \to \overline{\mathbb{F}_p}$ tali che $\beta_p(1) \neq 0$.



[25] Ricordiamo che, come detto prima, in $A[a^{-1}]$ il coefficiente di testa c_0 è invertibile.

[26] Ricordiamo che $\mathrm{GL}(n, A)$ è il gruppo delle matrici $n \times n$ invertibili a coefficienti in A, equivalentemente, a determinante invertibile.

$\operatorname{Ker}\beta_p$ è un ideale proprio di A; mostriamo che è massimale. Per prima cosa notiamo che $\operatorname{Ker}\beta_p \cap \mathbb{Z} = p\mathbb{Z}$, dove $\supset$ è ovvia e l'uguaglianza vale per massimalità, e chiaramente β_p induce una mappa iniettiva $A/\operatorname{Ker}\beta_p \to \overline{\mathbb{F}_p}$, che rende $A/\operatorname{Ker}_{\beta_p}$ una $\mathbb{F}_p$-algebra. Questa è finitamente generata da $\overline{a_1}, \dots \overline{a_m}$, e dato che $\overline{\mathbb{F}_p} = \bigcup_{s\in\mathbb{N}} \mathbb{F}_{p^s}$ si ha $\beta_p(\bar{a}_i) \in \mathbb{F}_{p^{s_i}}$ e se prendiamo $k = \operatorname{lcm}\{s_i \mid i \leq n\}$ l'immagine di A è contenuta in $\mathbb{F}_{p^k}$, per cui $A/\operatorname{Ker}\beta_p$ è finito, ed è un dominio perché vive in un campo. Dato che ogni dominio finito è un campo $\operatorname{Ker}\beta_p$ è, come anticipato, massimale.

Rinominiamo $\operatorname{Ker}\beta_p$ come $\mathfrak{m}_p$ e consideriamo l'omomorfismo di gruppi

$$\pi_p \colon \operatorname{GL}(n, A) \longrightarrow \operatorname{GL}(n, A/\mathfrak{m}_p)$$

che data una matrice $A = (a_{ij})$ restituisce la matrice $\overline{A} = (\overline{a_{ij}})$. Il suo nucleo $\operatorname{Ker}\pi_p$ è un sottogruppo normale di $\operatorname{GL}(n, A)$ e ha indice finito, perché $\operatorname{GL}(n, A)/\operatorname{Ker}\pi_p$ si immerge in un gruppo finito[27]. Dato ora Γ sottogruppo di $\operatorname{GL}(n, A)$ consideriamo $\Gamma_p = \Gamma \cap \operatorname{Ker}\pi_p$, che è sicuramente normale e di indice finito in Γ, perché Γ/Γ_p continua ad immergersi in un gruppo finito. Prendiamo un altro primo $q \neq p$ che non divide a e ripetiamo la costruzione, ottenendo così un sottogruppo $\Gamma_q = \Gamma \cap \operatorname{Ker}\pi_q$. Che il sottogruppo $\Gamma_p \cap \Gamma_q$ sia normale e di indice finito è immediato; mostriamo che è libero da torsione.

Sia per assurdo $g \in \Gamma_p \cap \Gamma_q$ una matrice tale che $g^r = \mathrm{id}$, e supponiamo WLOG r primo. Il polinomio minimo di g divide $t^r - 1$, che ha in $\mathbb{C}$ tutte radici distinte, per cui g è diagonalizzabile e ha come autovalori $\lambda_1, \dots, \lambda_n$ radici r-esime dell'unità. Inoltre uno dei λ_i deve essere una radice r-esima primitiva ζ_r, altrimenti g avrebbe ordine minore[28].

Consideriamo allora $B = A[\zeta_r]$, che è intero su A (è addirittura intero su $\mathbb{Z}$). Usando il Lying Over su $\mathfrak{m}_p \subseteq A$ otteniamo un ideale massimale $\mathfrak{n}_p \subseteq B$ tale che $\mathfrak{n}_p \cap A = \mathfrak{m}_p$. Sia $p_g(t)$ il polinomio caratteristico della matrice g; sappiamo che vale

$$p_g(t) \equiv (t-1)^n \pmod{\mathfrak{m}_p[t]}$$

cosa facile da vedere ricordandosi la definizione $p_g(t) = \det(tI - g)$ e che g vive in $\Gamma_p \cap \Gamma_q \subseteq \operatorname{Ker}\pi_p$. Dunque vale[29]

$$p_g(\zeta_r) \equiv (\zeta_r - 1)^n \pmod{\mathfrak{n}_p}$$

D'altra parte per definizione di autovalore deve valere $p_g(\zeta_r) = 0$. Dato che $B/\mathfrak{n}_p$ è un dominio e vale $(\zeta_r - 1)^n \equiv 0 \pmod{\mathfrak{n}_p}$, necessariamente $\zeta_r - 1 \in \mathfrak{n}_p$.

[27] Infatti, nel mostrare che $\operatorname{Ker}\beta_p$ è massimale, non solo abbiamo mostrato che $A/\mathfrak{m}_p$ è un campo, ma anche che è finito.

[28] E sarebbe l'identità perché, dato che abbiamo supposto r primo, tutte le $\zeta_r \neq 1$ sono primitive.

[29] Questo si vede "sostituendo ζ_r al posto di t" o, più formalmente, osservando che siccome $\mathfrak{m}_p[\zeta_r] = \mathfrak{m}_p^e = \mathfrak{n}_p^{ce} \subseteq \mathfrak{n}_p$ possiamo usare l'omomorfismo di valutazione $t \mapsto \zeta_r$ e passare al quoziente senza problemi.

Possiamo allora scrivere $\zeta_r = 1 + x$, per un certo $x \in \mathfrak{n}_p$. Abbiamo quindi

$$1 = \zeta_r^r = (1+x)^r = \sum_{j=0}^{r} \binom{r}{j} x^j = 1 + rx + x \underbrace{\left(\sum_{j=2}^{r} \binom{r}{j} x^{j-1} \right)}_{=y \in \mathfrak{n}_p} = 1 + x(r+y)$$

Dunque $x(r+y) = 0$, ma per costruzione $x \neq 0$. Poiché siamo in un dominio, $r = -y \in \mathfrak{n}_p \cap \mathbb{Z} = p\mathbb{Z}$, e dato che r è primo allora deve essere $r = p$. La stessa costruzione può però essere fatta con q, ottenendo l'assurdo $r = p \neq q = r$. □

Dimostrazione del Lemma di Selberg. Sia $\Gamma = \langle g_1, \dots, g_k \rangle$. Consideriamo le matrici $g_1, \dots, g_k, g_1^{-1}, \dots, g_k^{-1}$ e chiamiamo $a_1, \dots, a_m$ i coefficienti che compaiono in queste matrici. Per definizione di gruppo generato vale $\Gamma < \mathrm{GL}(n, \mathbb{Z}[a_1, \dots, a_m])$, e il Teorema precedente conclude. □

Dimostrazione del Teorema di Residuale Finitezza. Sia $g \in G < \mathrm{GL}(n, \mathbb{C})$, $g \neq 1$. Come fatto in precedenza, sia $A = \mathbb{Z}[a_1, \dots, a_m]$, dove $a_1, \dots a_m$ sono i coefficienti delle matrici che generano G. Supponiamo dapprima che la matrice g non sia diagonale, cioè che esista una sua entrata $b \neq 0$ fuori dalla diagonale. Prendiamo questo b come b del Teorema 1.48, ottenendo $a \in \mathbb{Z}$ come nella tesi. Prendiamo ora p tale che $p \nmid a$ e definiamo la proiezione $\pi_p \colon \mathrm{GL}(n, A) \to \mathrm{GL}(n, A/\mathfrak{m}_p)$ come nella dimostrazione del Teorema 1.49. Restringendo π_p otteniamo $\varphi_g \colon G \to \varphi_g(G)$ tale che $\varphi_g(g) \neq 1$, cosa che segue direttamente dal fatto che $\beta_p(b) \neq 0$ ripercorrendo le definizioni, e questo mostra che $\varphi_g(G)$ è finito perché vive dentro $\mathrm{GL}(n, A/\mathfrak{m}_p)$. Supponiamo invece che g sia una matrice diagonale non identica. Allora uno degli elementi sulla diagonale è della forma $1 + b$ e si ripete il ragionamento con tale b. □

Capitolo 2

Dimensione di Krull

2.1 Nelle Estensioni Intere

Come già detto il grado di trascendenza "si comporta come" una dimensione. In generale, per anelli arbitrari, si può definire un concetto di dimensione nella seguente maniera:

Definizione 2.1. Sia A un anello. La *dimensione di Krull* di A è

$$\dim(A) = \sup\{n \in \mathbb{N} \mid \text{esiste una catena di ideali primi } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n\}$$

La dimensione di un anello può anche essere infinita, per giunta anche nel caso noetheriano: anche se tutte le catene di primi sono finite basta che ne esistano di arbitrariamente lunghe. Effettivamente un anello del genere esiste e si chiama *controesempio di Nagata*, presentato nella Sezione 2.3. Anche se "senza saperlo", abbiamo praticamente già visto risultati sulla dimensione. Ad esempio

Proposizione 2.2. Sia $A \subseteq B$ un'estensione intera di anelli. Allora

$$\dim(A) = \dim(B)$$

Dimostrazione. Mostriamo prima che $\dim(A) \geq \dim(B)$. Consideriamo una catena di primi che realizza la dimensione di B:

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_n$$

Contraendo gli ideali, otteniamo una catena di primi in A e i contenimenti rimangono stretti per il Corollario 1.16, da cui $\dim(A) \geq n = \dim(B)$. L'altra disuguaglianza segue immediatamente dal Teorema del Going Up. □

2.2 Nelle $\mathbb{K}$-algebre

Per le $\mathbb{K}$-algebre che sono anche domini, abbiamo definito due nozioni: il grado di trascendenza su $\mathbb{K}$ e la dimensione di Krull. In realtà questi coincidono, cosa che dimostriamo subito occupandoci prima del caso particolare degli anelli di polinomi.

Teorema 2.3. Sia $A = \mathbb{K}[X_1, \dots, X_n]$ l'anello di polinomi su $\mathbb{K}$ in n variabili. Allora $\dim A = \operatorname{tr}_{\deg} A = n$.

Dimostrazione. Chiaramente $\operatorname{tr}_{\deg} A = n$. Dato che una catena di primi è

$$(0) \subsetneq (X_1), \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n)$$

abbiamo subito $\dim A \geq n$. Mostriamo l'altra disuguaglianza per induzione sul numero di variabili. Se $n = 1$, $\mathbb{K}[X]$ è un PID ma non un campo e quindi[1] ha dimensione 1. Procediamo al passo induttivo. Supponiamo di avere una catena di primi

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_m$$

e sia $0 \neq f \in \mathfrak{p}_1$ irriducibile[2]. Quozientiamo $\mathbb{K}[X_1, \dots, X_n]/(f) = B$ ottenendo

$$\mathfrak{p}_1/(f) \subsetneq \dots \subsetneq \mathfrak{p}_m/(f)$$

Dato che B è ancora una $\mathbb{K}$-algebra finitamente generata, per il LNN esistono $Y_1, \dots, Y_r$ algebricamente indipendenti tali che B è intero su $\mathbb{K}[Y_1, \dots, Y_r]$. Ma f è una relazione tra i generatori $\overline{X_i}$, per cui per l'Osservazione 1.29 $r < n$. Inoltre per il Corollario 1.16, la catena di primi $\mathfrak{p}_i/(f)$ dà una catena di $m-1$ primi distinti $\mathfrak{p}_i/(f) \cap \mathbb{K}[Y_1, \dots, Y_r]$. Dunque, usando la Proposizione 2.2 e l'ipotesi induttiva,

$$m - 1 \leq \dim B = \dim \mathbb{K}[Y_1, \dots, Y_r] = r < n \qquad \square$$

Teorema 2.4. Sia A una $\mathbb{K}$-algebra finitamente generata che è un dominio. Allora $\operatorname{tr}_{\deg} A = \dim A$.

Dimostrazione. Basta usare il LNN per scrivere A come estensione intera di $\mathbb{K}[Y_1, \dots, Y_r]$ e invocare il Teorema precedente e la Proposizione 2.2 ottenendo

$$\operatorname{tr}_{\deg} A = r = \dim \mathbb{K}[Y_1, \dots, Y_r] = \dim A \qquad \square$$

Cosa ci facciamo con la dimensione? Ad esempio ci potremmo volere fare le dimostrazioni per induzione, con l'idea intuitiva che quozientare in maniera sensata, dato che "uccide" degli ideali, dovrebbe far calare la dimensione, e prestarsi come passo induttivo. Effettivamente questo accade spesso; entriamo più nel dettaglio.

[1] Se $(a) \subseteq (b)$ sono due primi e $a \neq 0$ è facile mostrare che b deve essere della forma ka, con k invertibile.

[2] Usando il fatto che A è un UFD, se fattorizziamo in irriducibili $p = \prod p_i^{\alpha_i} \in \mathfrak{p}_1$, per primalità esiste un $p_i \in \mathfrak{p}_1$ e possiamo sceglierlo come f.

Definizione 2.5. Sia $\mathfrak{p} \in \operatorname{Spec} A$. L'*altezza* di $\mathfrak{p}$ è la dimensione di Krull di $A_\mathfrak{p}$ e si denota con $\operatorname{ht}(\mathfrak{p})$. La sua *profondità* è la dimensione di $A/\mathfrak{p}$, e si denota con $\operatorname{depth}(\mathfrak{p})$.

Proposizione 2.6. Sia $S = \mathbb{K}[x_1, \dots, x_m]$ un dominio con $\dim S = n$ e sia $\mathfrak{p}$ un primo di altezza 1. Allora $\dim S/\mathfrak{p} = n - 1$.

Dimostrazione. Supponiamo prima di trovarci fra le mani un anello di polinomi $S = \mathbb{K}[X_1, \dots, X_n]$. Dato che $\operatorname{ht}(\mathfrak{p}) = 1$ si ha $\mathfrak{p} = (f)$, con f irriducibile, perché altrimenti preso f irriducibile in $\mathfrak{p}$ riusciremmo a scrivere $0 \subsetneq (f) \subsetneq \mathfrak{p}$. Possiamo dunque scrivere (a meno di cambiare nome alle variabili)

$$f = f_r(X_2, \dots, X_n)X_1^r + \dots + f_0(X_2, \dots, X_n) = \sum_{j=0}^{r} f_j(X_2, \dots, X_n)X_1^j$$

e notare subito che $\mathbb{K}[X_2, \dots, X_n] \cap (f) = \{0\}$. Dato che (f) è il nucleo della proiezione al quoziente in $S/(f) = S/\mathfrak{p}$, $\mathbb{K}[X_2, \dots, X_n]$ si immerge in $S/\mathfrak{p}$, e indichiamo la sua immagine con $\mathbb{K}[\overline{X_2}, \dots, \overline{X_n}]$. Qui abbiamo almeno $n-1$ elementi algebricamente indipendenti, gli $\overline{X_2}, \dots, \overline{X_n}$, e dunque $\dim S/\mathfrak{p} \geq n - 1$. D'altra parte, per il LNN e l'Osservazione 1.29, dato che f è una relazione fra $\overline{X_1}, \dots, \overline{X_n}$, abbiamo $\dim S/\mathfrak{p} < n$.

In generale, via LNN, possiamo supporre che S sia intero su $\mathbb{K}[Y_1, \dots, Y_r]$, dove in realtà $r = n$, perché come mostrato nella Proposizione 2.2 le estensioni intere preservano la dimensione. Denotando $\mathfrak{p}_0 = \mathfrak{p} \cap \mathbb{K}[Y_1, \dots, Y_r]$, abbiamo che $S/\mathfrak{p}$ è intero su $\mathbb{K}[Y_1, \dots, Y_r]/\mathfrak{p}_0$, e quindi ha la stessa dimensione. Se riuscissimo a dire che $\operatorname{ht}(\mathfrak{p}_0) = 1$ questa sarebbe $n - 1$ per la prima parte della dimostrazione e avremmo concluso. Ma questo segue dal Teorema del Going Down, che può essere utilizzato perché $\mathbb{K}[Y_1, \dots, Y_r]$ è un UFD e quindi è integralmente chiuso[3]. □

Definizione 2.7. Un anello R si dice *catenario* se, comunque dati due primi $\mathfrak{p} \subsetneq \mathfrak{p}'$, tutte le catene massimali di primi fra $\mathfrak{p}$ e $\mathfrak{p}'$ hanno la stessa lunghezza.

Teorema 2.8. Ogni $\mathbb{K}$-algebra finitamente generata S è catenaria e ogni catena massimale di primi da $\mathfrak{p}$ a $\mathfrak{p}'$ ha lunghezza $\operatorname{depth}(\mathfrak{p}) - \operatorname{depth}(\mathfrak{p}')$.

Dimostrazione. Sia $\mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r = \mathfrak{p}'$ una catena massimale. Consideriamo[4]

$$S\!\!\diagup_{\mathfrak{p}} \twoheadrightarrow S\!\!\diagup_{\mathfrak{p}_1} \twoheadrightarrow \dots \twoheadrightarrow S\!\!\diagup_{\mathfrak{p}_r} = S\!\!\diagup_{\mathfrak{p}'}$$

Questi sono tutti domini e in ogni passaggio, per massimalità della catena, stiamo quozientando per un primo di altezza 1, e quindi la dimensione cala di 1 ad ogni freccia per la Proposizione precedente. Quindi

$$r = \dim S\!\!\diagup_{\mathfrak{p}} - \dim S\!\!\diagup_{\mathfrak{p}'} = \operatorname{depth}(\mathfrak{p}) - \operatorname{depth}(\mathfrak{p}') \qquad \square$$

[3] Vedi Esempio 1.2.

[4] Se una freccia ha due teste ($\twoheadrightarrow$) vuol dire che è surgettiva.

Corollario 2.9. Se S è anche un dominio gli ideali massimali hanno tutti la stessa altezza.

Dimostrazione. Dire che S è un dominio vuol dire che (0) è un ideale primo. Fissiamo $\mathfrak{m}$ massimale e abbiamo

$$\operatorname{ht}(\mathfrak{m}) = \dim {}^{S}\!/_{(0)} - \dim {}^{S}\!/_{\mathfrak{m}} = \dim S - \dim {}^{S}\!/_{\mathfrak{m}} = \dim S$$

perché $S/\mathfrak{m}$ è un campo, e quindi[5] ha dimensione 0. □

In contesto "geometria algebrica" stiamo dicendo che se l'anello coordinato è un dominio, cioè la varietà è irriducibile, in ogni punto di questa la dimensione è la stessa[6]. Se S non è un dominio possono presentarsi alcuni problemi:

Controesempio 2.10. Consideriamo in $S = \mathbb{K} \times \mathbb{K}[X_1, \dots, X_n]$ gli ideali massimali $\mathfrak{m}_1 = (0) \times \mathbb{K}[X_1, \dots, X_n]$ e $\mathfrak{m}_2 = \mathbb{K} \times (X_1, \dots, X_n)$. È chiaro che $0 = \operatorname{ht}(\mathfrak{m}_1) \neq \operatorname{ht}(\mathfrak{m}_2) = n$.

Del resto che in $\mathbb{K}$-algebre che non sono domini le cose tendono a funzionare male l'avevamo visto già nel Controesempio 1.35.

Esercizio 2.11. Sia $R = \mathbb{K}[X] \times \mathbb{K}[Y]$. Calcolarne la dimensione di Krull e capire se esiste un insieme algebricamente indipendente di cardinalità 2.

Esempio 2.12. Sia R l'anello locale $\mathbb{Z}_{(p)}$, con p primo, e consideriamo $\frac{p}{1} = t$ il generatore dell'ideale massimale di R. Guardiamo in $R[X]$ i massimali $\mathfrak{m}_1 = (tX - 1)$ e $\mathfrak{m}_2 = (t, X)$.

Che sono massimali si vede quozientando (e usando il Lemma di Gauss a un certo punto per $\mathfrak{m}_1$). Questi due massimali hanno altezze diverse: infatti $\operatorname{ht}(\mathfrak{m}_1) \leq 1$, perché $\mathfrak{m}_1$ è generato da un solo elemento, e

Proposizione 2.13. In un anello noetheriano ogni primo strettamente contenuto in un ideale principale ha altezza 0.

Dimostrazione. Supponiamo $\mathfrak{q} \subsetneq \mathfrak{p} \subsetneq (x)$, e per prima cosa, quozientando per $\mathfrak{q}$, ci riconduciamo al caso $(0) \subsetneq \mathfrak{p} \subsetneq (x)$ in un dominio. Ora un qualunque $y \in \mathfrak{p}$ si scrive come $y = ax$ e siccome $x \notin \mathfrak{p}$ abbiamo $a \in \mathfrak{p}$, per cui $\mathfrak{p} = \mathfrak{p}x$. Per Cayley-Hamilton esiste $b \in (x)$ tale che $(1 - b)\mathfrak{p} = 0$. Poiché siamo in un dominio abbiamo $1 - b = 0$, e quindi $1 \in (x)$, che è assurdo. □

[5] Banalmente, il suo unico primo è (0) e non è che ci si possano fare catene particolarmente lunghe.

[6] Nel senso, detto molto male, che ad esempio una varietà irriducibile non può "cambiare dimensione" (si pensi a una retta incollata a un piano a cui non appartiene). Chi è interessato ad approfondire può dare un'occhiata a [14].

Quant'è invece $\mathrm{ht}(\mathfrak{m}_2)$? Sicuramente è almeno 2 perché $(0) \subsetneq (X) \subsetneq \mathfrak{m}_2$, e questo ci basta[7]. Dunque $R[X]$ sembra tanto un bell'oggetto, nel senso che per esempio è noetheriano, ma fa comunque questi "scherzi". Magari uno non se l'aspettava.

Esercizio 2.14 (Lampo)**.** Sia[8] $A = \mathbb{K}[X^2, X^3]$. Dimostrare che gli ideali primi non nulli hanno altezza 1.

Soluzione. $\mathbb{K}[X]$ è intero su A perché X soddisfa il polinomio $t^3 - X^3 \in \mathbb{K}[X^2, X^3][t]$. Ma allora $\dim A = 1$, e dato che siamo in un dominio (0) è primo e tutti gli altri primi non possono che avere altezza 1. □

Esercizio 2.15. Trovare la chiusura integrale di $R = \mathbb{K}[X, Y]/(Y^3 - X^5)$ dentro il suo campo delle frazioni.

Intanto bisogna vedere che R è un dominio, sennò non ha senso parlare di campo delle frazioni, ma $Y^3 - X^5$ è irriducibile e quindi primo. Per l'irriducibilità, se proprio non abbiamo idee furbe, si può fare via forza bruta: uno lo vede come polinomio in $(\mathbb{K}[X])[Y]$, lo prova a fattorizzare e scopre che dovrebbe essere della forma $(Y - p(X))(Y^2 + \ldots)$. Dunque, come polinomio in $(\mathbb{K}(X))[Y]$, dovrebbe avere una radice $q(X)/s(X)$. Ne seguirebbe $q(X)^3 = X^5 s(X)^3$, e ci sono problemi di congruenza modulo 3 sui gradi dei polinomi.

Soluzione. Consideriamo l'isomorfismo $R \cong \mathbb{K}[T^3, T^5]$ indotto dall'omomorfismo $\vartheta\colon \mathbb{K}[X, Y] \to \mathbb{K}[T^3, T^5]$ definito da $X \mapsto T^3$ e $Y \mapsto T^5$. L'unica cosa non ovvia da mostrare è $\operatorname{Ker}\vartheta \subseteq (Y^3 - X^5)$. Usando la teoria della dimensione è immediato: altrimenti avremmo

$$(0) \subsetneq (Y^3 - X^5) \subsetneq \operatorname{Ker}\vartheta$$

e $\operatorname{Ker}\vartheta$ è primo ma *non* massimale, perché il quoziente è un dominio ma non un campo. Dunque $\mathbb{K}[X, Y]$ dovrebbe avere dimensione almeno 3, ma sappiamo che non è così.

Ci siamo dunque ricondotti a cercare la chiusura integrale C di $\mathbb{K}[T^3, T^5]$ nel suo campo delle frazioni, che per gli amici è $\mathbb{K}(T)$, perché possiamo scrivere $T = (T^3)^2/T^5$. Notiamo che T è intero su $\mathbb{K}[T^3, T^5]$ perché soddisfa il polinomio $\lambda^3 - T^3$, e quindi $\mathbb{K}(T) \supseteq C \supseteq \mathbb{K}[T]$. Quest'ultimo però è integralmente chiuso in quanto UFD[9]. □

[7] Per ora; a titolo di cronaca è vero che fa 2, perché vedremo che se R è noetheriano di dimensione n allora $R[x]$ ha dimensione $n + 1$. Vedi Teorema 5.34. Una motivazione alternativa è presentata dopo il Corollario 5.17.

[8] Ora la notazione "esplode", nel senso che quella X è proprio quella dei polinomi, anche se effettivamente fra X^2 e X^3 ci sono relazioni e quindi magari avremmo dovuto usare la minuscola... comunque ci siamo capiti.

[9] Vedi Esempio 1.2.

Esercizio 2.16. Nell'Esercizio 1.25 calcolare la dimensione di A.

Soluzione. Come già visto nell'Esercizio 1.25 l'anello che stiamo studiando è "in realtà" $S^{-1}\mathbb{Z}[\sqrt{-3}]$, dove $S = \{2^i \mid i \in \mathbb{N}\}$, che è un'estensione intera di $S^{-1}\mathbb{Z}$ perché la localizzazione si comporta bene con le estensioni intere[10]. Quindi il nostro anello ha la stessa dimensione di $S^{-1}\mathbb{Z}$. Qui però sappiamo che i primi sono "i primi di $\mathbb{Z}$ che non intersecano S", e quindi la dimensione è 1. □

2.3 Il Controesempio di Nagata

In questa sezione costruiamo il Controesempio di Nagata, un dominio noetheriano di dimensione infinita. L'idea è partire da $B = \mathbb{C}[x_1, x_2, \ldots]$, l'anello dei polinomi complessi in $\aleph_0$ variabili, e "farlo diventare" noetheriano passando ad un opportuno anello di frazioni. Nel dettaglio, si considerano i primi[11]

$$\mathfrak{p}_1 = (x_1), \mathfrak{p}_2 = (x_2, x_3), \ldots, \mathfrak{p}_i = \left(x_{\binom{i}{2}+1}, \ldots, x_{\binom{i+1}{2}}\right), \ldots$$

Dopodiché si definisce $S_i = B \setminus \mathfrak{p}_i$ e si pone

$$S = \bigcap_{i \in \mathbb{N}} S_i = B \setminus \bigcup_{i \in \mathbb{N}} \mathfrak{p}_i$$

L'anello cercato è $A = S^{-1}B$; questo è un dominio perché B lo è e $0 \notin S$.

Claim. A ha dimensione infinita.

Dimostrazione. Dato che più è grande S più primi muoiono, per ogni i da $S \subseteq S_i$ otteniamo

$$\dim A = \dim S^{-1}B \geq \dim S_i^{-1}B$$

Chiaramente se mostriamo che $\forall i \in \mathbb{N}\ \dim S_i^{-1}B \geq i$ abbiamo finito. Se $\mathfrak{p}_i = (x_n, \ldots, x_k)$, con $k - n = i$, scriviamo $S_i^{-1}B$ come

$$\mathbb{C}(x_1, \ldots, x_{n-1}, x_{k+1}, \ldots)[x_n, \ldots, x_k]_{(x_n,\ldots,x_k)} = \mathbb{K}[x_n, \ldots, x_k]_{(x_n,\ldots,x_k)}$$

ed è palese che qui dentro c'è la catena lunga i

$$(0) \subsetneq (x_n) \subsetneq (x_n, x_{n+1}) \subsetneq \ldots \subsetneq (x_n, \ldots, x_k)$$ □

Claim. A è noetheriano.

Mostrare questo è più laborioso, e richiede questi due risultati:

[10] Vedi Proposizione 1.10.

[11] Per comodità psicologica di chi ha paura dei binomiali: $\mathfrak{p}_i$ è generato da i elementi.

Lemma 2.17. Siano $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ primi di R e I un qualsiasi suo ideale. Allora se $I \subseteq \bigcup \mathfrak{p}_i$ esiste i tale che $I \subseteq \mathfrak{p}_i$

Lemma 2.18. Se R è tale che

1. Per ogni $\mathfrak{m} \in \operatorname{SpecMax} R$ il localizzato $R_{\mathfrak{m}}$ è noetheriano.
2. Ogni $0 \neq f \in R$ è contenuto in un numero finito di ideali massimali.

allora R è noetheriano.

Il Lemma 2.17 fa parte dei risultati noti da Algebra 2[12], e quindi non lo dimostriamo. Prima di dimostrare il Lemma 2.18 vediamo come si conclude.

Dimostrazione che A è noetheriano. Chi sono i massimali di A? Mostriamo che tutti gli $\mathfrak{a}_i = S^{-1}\mathfrak{p}_i$ sono massimali. Supponiamo che[13] $\mathfrak{a}_i \subseteq S^{-1}I$, dove $I \supseteq \mathfrak{p}_i$ e $I \cap S = \emptyset$, e sia per assurdo $f \in I \setminus \mathfrak{p}_i$. Scriviamo

$$f = g(\text{variabili non in } \mathfrak{p}_i) + \underbrace{h_i}_{\in \mathfrak{p}_i}$$

dove $g \neq 0$ perché $f \notin \mathfrak{p}_i$. Dato che $\mathfrak{p}_i \subseteq I$ abbiamo $g = f - h_i \in I$. Dato che $x_n \in \mathfrak{p}_i \subseteq I$ si ha allora $g + x_n \in I$, ma d'altra parte $g + x_n \notin \mathfrak{p}_i$, perché altrimenti g, e di conseguenza f, starebbe in $\mathfrak{p}_i$. Siccome anche per $j \neq i$ si ha[14] $g + x_n \notin \mathfrak{p}_j$ abbiamo $g + x_n \in S$. Questo vuol dire che $g + x_n \in I \cap S$, che però dovrebbe essere vuoto.

Mostriamo che non ce ne sono altri. Preliminarmente, ponendo $\tilde{\mathfrak{p}}_\ell = (\mathfrak{p}_{\ell+1}, \mathfrak{p}_{\ell+2}, \ldots)$, che è primo perché il quoziente è un dominio, abbiamo

$$T_\ell = B \setminus \left[\bigcup_{j=1}^{\ell} \mathfrak{p}_j \cup \tilde{\mathfrak{p}}_\ell \right] \subseteq S$$

Gli unici ideali massimali di $T_\ell^{-1}B$ sono $T_\ell^{-1}\mathfrak{p}_1, \ldots, T_\ell^{-1}\mathfrak{p}_\ell$ e $T_\ell^{-1}\tilde{\mathfrak{p}}_\ell$: infatti se abbiamo $T_\ell^{-1}I$, con $I \cap T_\ell = \emptyset$, per il Lemma 2.17 allora I è incluso in $\tilde{\mathfrak{p}}_\ell$ o in uno dei $\mathfrak{p}_j$. Finita questa chiacchierata preliminare, sia $S^{-1}I$ un ideale di A, con $I \cap S = \emptyset$, e mostriamo che per un qualche j si ha $I \subseteq \mathfrak{p}_j$. Se $I = (0)$ non c'è niente da dimostrare, altrimenti sia $0 \neq f \in I$. In f compariranno un numero finito di variabili, che supponiamo reperibili in $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$. Dato che $T_\ell \subseteq S$ abbiamo $I \cap T_\ell = \emptyset$, e per la chiacchierata basta escludere che sia $I \subseteq \tilde{\mathfrak{p}}_\ell$. Ma per definizione di ℓ abbiamo $f \notin \tilde{\mathfrak{p}}_\ell$, per cui $I \subseteq \mathfrak{p}_j$ per un qualche $j \leq \ell$, e questo prova che non ci sono altri massimali di A al di fuori degli $\mathfrak{a}_i$.

[12] Comunque è nel primo capitolo di [2], dove si chiama Proposizione 1.11..

[13] Ricordiamo che tutti gli ideali degli anelli di frazioni sono ideali estesi.

[14] Basta ricordarsi la definizione dei $\mathfrak{p}_j$ e il fatto che in g non ci sono termini che possano cancellare x_n.

Ora però $A_{\mathfrak{a}_i} = S_i^{-1}B = \mathbb{K}[x_n, \ldots, x_k]_{(x_n,\ldots,x_k)}$ è noetheriano e ogni $0 \neq f \in A$ appartiene solo a finiti $\mathfrak{a}_i$ perché in f compaiono solo un numero finito di variabili, per cui scatta il Lemma 2.18 e abbiamo la tesi. □

Per completare il quadro ci resta solo da affrontare la

Dimostrazione del Lemma 2.18. Quello che mostriamo è che ogni ideale I di R è finitamente generato. Se $I = (0)$ non c'è nulla da fare, altrimenti sia $0 \neq f \in I$. Per ipotesi esistono finiti massimali $\mathfrak{m}_1, \ldots, \mathfrak{m}_a$ cui f appartiene. Sempre per ipotesi i localizzati per gli $\mathfrak{m}_j$ sono noetheriani, per cui i loro ideali sono finitamente generati, e in particolare sarà $I_{\mathfrak{m}_j} = (f_{j_1}, \ldots, f_{j_{b_j}})_{\mathfrak{m}_j}$. Per concludere basta mostrare che l'unione I_1 di tutti questi generatori e di f basta a generare I, cioè la nostra tesi diventa

$$I = \left(f, \bigcup_{j=1}^{a} \{f_{j_1}, \ldots, f_{j_{b_j}}\} \right) = I_1$$

Dato che $\supseteq$ è ovvia, ci basta mostrare che se $g \in I$ allora posto $J = \{h \mid hg \in I_1\}$ si ha $J = R$, perché $1 \in J \Rightarrow g \in I_1$. Dato che J è un ideale, supponiamo per assurdo che esista un massimale $\mathfrak{m} \supseteq J$. Un tale $\mathfrak{m}$ deve essere uno degli $\mathfrak{m}_j$, perché $f \in J$ e non ci sono altri massimali che contengono f, e possiamo supporre WLOG $\mathfrak{m} = \mathfrak{m}_1$. Localizzando otteniamo $J_{\mathfrak{m}_1} \subseteq \mathfrak{m}_{1\mathfrak{m}_1} \neq R_{\mathfrak{m}_1}$, contro il fatto che, srotolando le definizioni,

$$J_{\mathfrak{m}_1} = \{h \in R_{\mathfrak{m}_1} \mid hg \in \underbrace{I_{1\mathfrak{m}_1}}_{=I_{\mathfrak{m}_1} \ni g} \} = R_{\mathfrak{m}_1}$$ □

2.4 La Noetherianità è Locale?

Oltre a esserci servito nella costruzione di A, il Lemma 2.18 ci dice che sotto opportune ipotesi la noetherianità è una proprietà locale, visto che è facile mostrare che, anche senza le ipotesi del Lemma,

Esercizio 2.19. Se A noetheriano allora per ogni $\mathfrak{p} \in \operatorname{Spec} A$ anche $A_{\mathfrak{p}}$ è noetheriano.

Dimostrazione. Basta ricordare che gli ideali di un anello di frazioni sono tutti ideali estesi. □

Comunque per anelli qualunque la noetherianità *non* è una proprietà locale: per passare dai localizzati all'anello di partenza qualche ipotesi serve, come mostra il seguente

Controesempio 2.20. $A = \prod_{i=1}^{\infty} \mathbb{K}$, con $\mathbb{K}$ campo, non è noetheriano, ma tutti i suoi localizzati lo sono.

Dimostrazione. Basta prendere la catena degli ideali del tipo "le coordinate dalla n-esima in poi sono nulle". Se però $\mathfrak{p} \in \operatorname{Spec} A$, sia $a/b \in A_{\mathfrak{p}}$. Se $a \notin \mathfrak{p}$ allora a/b è invertibile, altrimenti deve avere una qualche coordinata nulla, per cui l'elemento "cattivo" c dato dall'indicatrice delle coordinate nulle di a è non nullo. Deve essere $c \notin \mathfrak{p}$, altrimenti $a + c \in \mathfrak{p}$, che è assurdo perché $a + c$ è invertibile. Otteniamo quindi

$$\frac{a}{b} = \frac{ac}{bc} = 0$$

Abbiamo quindi mostrato che a/b è invertibile oppure è 0, cioè $A_{\mathfrak{p}}$ è un campo, e quindi noetheriano. □

Capitolo 3

Catene, Lunghezze, Graduati

3.1 Caratterizzazione degli Anelli Artiniani

La condizione di artinianità è la condizione di noetherianità "al contrario", cioè con le inclusioni rovesciate. Più formalmente

Definizione 3.1. Un anello si dice *artiniano* se verifica la *descending chain condition (d.c.c.)*, cioè se ogni catena discendente di ideali $I_0 \supseteq I_1 \supseteq \dots$ è definitivamente costante. Equivalentemente, se ogni famiglia non vuota di ideali, ordinata per inclusione, ha un elemento minimale. Un modulo si dice artiniano se valgono le stesse condizioni di sopra rimpiazzando "ideali" con "sottomoduli".

Scopo di questa sezione è dimostrare (spoiler) che gli anelli artiniani sono tutti e soli i noetheriani di dimensione 0. Daremo per buoni[1] i seguenti fatti:

Proposizione 3.2. Negli anelli artiniani

- Ogni ideale primo è massimale.
- Gli ideali massimali sono in numero finito

Proposizione 3.3. Sia I un ideale di un anello noetheriano. Allora esiste $n \in \mathbb{N}$ tale che $(\sqrt{I})^n \subseteq I$.

In particolare in un anello noetheriano il nilradicale è nilpotente. La prima cosa che dimostriamo è che questo è vero anche negli anelli artiniani.

Proposizione 3.4. In ogni anello artiniano il nilradicale $\mathcal{R}$ è nilpotente.

[1] Perché sono stati dimostrati nel corso di Algebra 2. In ogni caso le dimostrazioni possono essere reperite in [2] cercando, nell'ordine, Proposizione 8.1, Proposizione 8.3 e Proposizione 7.14.

Dimostrazione. Per artinianità esiste $k \in \mathbb{N}$ tale che

$$\mathcal{R} \supseteq \mathcal{R}^2 \supseteq \ldots \supseteq \mathcal{R}^k = \mathcal{R}^{k+1} = \mathfrak{a}$$

Supponiamo per assurdo che $\mathfrak{a} \neq \{0\}$. Consideriamo l'insieme

$$\Sigma = \{\mathfrak{b} \text{ ideale} \mid \mathfrak{a}\mathfrak{b} \neq 0\}$$

che è non vuoto perché $\mathcal{R} \in \Sigma$ per scelta di $\mathfrak{a}$. Per artinianità, esiste allora un ideale $\mathfrak{c} \in \Sigma$ minimale. Dato che $\mathfrak{c}\mathfrak{a} \neq 0$, esiste $x \in \mathfrak{c}$ tale che $x\mathfrak{a} \neq 0$. Di conseguenza, $(x)\mathfrak{a} \neq 0$ e per minimalità $\mathfrak{c} = (x)$. Inoltre $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$, quindi sempre per minimalità $(x)\mathfrak{a} = (x)$, per cui esiste $y \in \mathfrak{a}$ tale che $xy = x$. Ne segue

$$x = xy = xy^2 = \ldots = xy^n = \ldots$$

e dato che $y \in \mathfrak{a} \subset \mathcal{R}$ per n abbastanza grande $y^n = 0$, e quindi $x = 0$. Questo è assurdo perché allora $(0) \neq \mathfrak{c}\mathfrak{a} = (0)\mathfrak{a} = (0)$. □

L'ultimo risultato che ci serve per la classificazione è il seguente.

Lemma 3.5. Sia A un anello e supponiamo che (0) si scriva come prodotto finito di ideali massimali (anche con ripetizione). Allora A è noetheriano se e solo se è artiniano.

Dimostrazione. Siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ gli ideali massimali tali che $\prod \mathfrak{m}_i = (0)$ e scriviamo

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \ldots \supseteq \prod \mathfrak{m}_i = (0)$$

Consideriamo i quozienti

$$A/\mathfrak{m}_1,\ \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2,\ \mathfrak{m}_1\mathfrak{m}_2/\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3, \ldots, \left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right) \Big/ \underbrace{\left(\prod_{i=1}^{r} \mathfrak{m}_i\right)}_{=(0)}$$

che sono spazi vettoriali[2] sui campi $A/\mathfrak{m}_1$, $A/\mathfrak{m}_2$, etc. Quindi per ognuno di loro vale la d.c.c. se e solo se vale la a.c.c, perché "sottomodulo" in uno spazio vettoriale vuol dire "sottospazio", e entrambe le chain conditions sono[3] equivalenti al fatto che lo spazio sia di dimensione finita. Inoltre, i sottospazi come $A/\mathfrak{m}_i$-spazi vettoriali coincidono con i sottomoduli come A-moduli[4]. Ora, in una successione esatta di A-moduli il termine centrale è

[2] Dove la moltiplicazione per scalare è la prima sensata che vi viene in mente.

[3] Ognuna per conto suo.

[4] Basta pensarci un attimo (o provare a scrivere entrambe le moltiplicazioni per scalare) per convincersene.

noetheriano/artiniano se e solo se lo sono gli altri due[5] per cui, partendo da $0 \to \mathfrak{m}_1 \to A \to A/\mathfrak{m}_1 \to 0$ e guardandosi tutte le successioni del tipo

$$0 \to \prod_{i=1}^{j} \mathfrak{m}_i \to \prod_{i=1}^{j-1} \mathfrak{m}_i \to \left(\prod_{i=1}^{j-1} \mathfrak{m}_i\right) \Big/ \left(\prod_{i=1}^{j} \mathfrak{m}_i\right) \to 0$$

ci accorgiamo che A è noetheriano/artiniano se e solo se tutti i quozienti di sopra sono noetheriani/artiniani[6]. In conclusione abbiamo

A noetheriano $\Leftrightarrow$ quozienti noetheriani $\Leftrightarrow$ quozienti artiniani $\Leftrightarrow$ A artiniano □

Teorema 3.6 (Caratterizzazione degli Anelli Artiniani)**.** Sia A un anello. Sono equivalenti:

- A è artiniano
- A è noetheriano di dimensione 0

Dimostrazione. Se A è artiniano sappiamo già che ha dimensione 0 dalla Proposizione 3.2. Siano, per le Proposizioni precedenti, $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ gli ideali massimali di A e k tale che $\mathcal{R}^k = (0)$. Abbiamo

$$\prod \mathfrak{m}_i^k = \left(\prod \mathfrak{m}_i\right)^k \subseteq \left(\bigcap \mathfrak{m}_i\right)^k = \mathcal{R}^k = (0) \tag{3.1}$$

E per il Lemma precedente A è noetheriano.

Viceversa, sia A noetheriano di dimensione 0. Per noetherianità (0) ammette una decomposizione primaria; i primi associati $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ sono i primi minimali[7] di A, ma dato che $\dim A = 0$ questi sono anche massimali,

[5] È facile, comunque è sempre su [2], Proposizione 6.3.

[6] Ad esempio, assumendo A noetheriano e partendo da

$$0 \to \mathfrak{m}_1 \to A \to A/\mathfrak{m}_1 \to 0$$

si ottiene $\mathfrak{m}_1$ noetheriano (e $A/\mathfrak{m}_1$, ma in questo caso è gratis perché è un campo), per cui se scriviamo

$$0 \to \mathfrak{m}_1\mathfrak{m}_2 \to \mathfrak{m}_1 \to \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2 \to 0$$

otteniamo la noetherianità del quoziente, ma anche di $\mathfrak{m}_1\mathfrak{m}_2$, il che permette di reiterare il processo. Viceversa assumendo che tutti i quozienti siano noetheriani e partendo da

$$0 \to \underbrace{\left(\prod_{i=1}^{r} \mathfrak{m}_i\right)}_{=(0)} \to \left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right) \to \underbrace{\left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right) \Big/ \left(\prod_{i=1}^{r} \mathfrak{m}_i\right)}_{=\left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right)} \to 0$$

si ha la noetherianità del termine centrale, che però è il termine di sinistra di

$$0 \to \left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right) \to \left(\prod_{i=1}^{r-2} \mathfrak{m}_i\right) \to \left(\prod_{i=1}^{r-2} \mathfrak{m}_i\right) \Big/ \left(\prod_{i=1}^{r-1} \mathfrak{m}_i\right) \to 0$$

e, dato che il termine di destra è noetheriano per ipotesi, lo è anche quello centrale. Questo permette di iterare il processo "risalendo" fino ad A.

[7] Vedi sempre [2], Proposizione 4.6. e Teorema 7.13.

per cui A non ha altri ideali primi, perché per ogni $\mathfrak{p}$ esiste $\mathfrak{p}_i$ tale che $\mathfrak{p} \supseteq \mathfrak{p}_i$, e per massimalità $\mathfrak{p} = \mathfrak{p}_i$. Se li ribattezziamo $\mathfrak{m}_i$ però abbiamo di nuovo la (3.1), che fa scattare il Lemma precedente, per cui da A noetheriano segue A artiniano. □

Esistono anelli di dimensione 0 non noetheriani? Sì, e ne abbiamo già incontrato uno nel Controesempio 2.20: dato che tutti i suoi localizzati sono campi le catene di primi non possono essere particolarmente lunghe. Un esempio di sua catena discendente infinita è data dagli ideali del tipo "le prime n coordinate sono nulle".

Per gli anelli artiniani esiste anche un Teorema di Struttura, che ci limitiamo ad enunciare, ma la cui dimostrazione può essere reperita in [2], dove si chiama Teorema 8.7.

Teorema 3.7 (di Struttura degli Anelli Artiniani)**.** Ogni anello artiniano si scrive in maniera unica (a meno di isomorfismo) come prodotto diretto di un numero finito di anelli artiniani locali.

3.2 Serie di Composizione

Definizione 3.8. Sia M un A-modulo. Una *catena finita di sottomoduli* è una successione di sottomoduli del tipo

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = 0$$

ed n è detta *lunghezza* della catena. Una catena massimale, cioè nella quale M_i/M_{i+1} non ha sottomoduli non banali, è detta *serie di composizione.*

Teorema 3.9. Supponiamo che M ammetta una serie di composizione di lunghezza n. Allora ogni serie di composizione ha lunghezza n e ogni catena in M può essere estesa ad una serie di composizione.

Dimostrazione. Sia $\ell(M)$ la lunghezza minima di una serie di composizione in M, che è un numero finito per ipotesi. La dimostrazione si articola su tre passi:

1. Se $N \subsetneq M$ allora $\ell(N) < \ell(M)$.
2. Ogni catena in M ha lunghezza $\leq \ell(M)$.
3. Dimostrazione del Teorema.

1. Sia $M = M_0 \supsetneq \ldots \supsetneq M_k = 0$ una serie di composizione di lunghezza minima, e definiamo $N_i = N \cap M_i$. Otteniamo così la catena

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = 0$$

Ogni N_i/N_{i+1} è però un A-sottomodulo di M_i/M_{i+1}, che per ipotesi non ha sottomoduli non banali, per cui o $N_i/N_{i+1} = 0$ e siamo in presenza di una "ripetizione", oppure $N_i/N_{i+1} = M_i/M_{i+1}$, il contenimento $N_i \supseteq N_{i+1}$ è stretto e N_i/N_{i+1} non ha sottomoduli non banali. Eliminando le "ripetizioni" otteniamo quindi una serie di composizione per N, per cui $\ell(N)$ è ben definita e $\ell(N) \leq \ell(M)$. Se fosse $\ell(N) = \ell(M)$, da $M_{k-1}/0 = N_{k-1}/0$ otteniamo $N_{k-1} = M_{k-1}$. Ma allora abbiamo $M_{k-2}/M_{k-1} = N_{k-2}/N_{k-1}$, i moduli per cui quozientiamo sono uguali e $N_{k-2} \subseteq M_{k-2}$, per cui otteniamo $N_{k-2} = M_{k-2}$. Iterando si "risale" fino a $M = N$, contro le ipotesi.

2. Applicando il passo precedente agli "anelli[8]" di una catena

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_k = 0$$

otteniamo $\ell(M) > \ell(M_1) > \ldots > \ell(M_k) = 0$, per cui $\ell(M) \geq k$.

3. Presa una serie di composizione di M questa ha lunghezza $k \leq \ell(M)$ per il passo precedente, e per definizione di $\ell(M)$, che è il minimo delle lunghezze delle serie di composizione, si ha $k = \ell(M)$. Per il punto precedente ogni catena (M_i) ha lunghezza $\leq \ell(M)$. Se questa è effettivamente $\ell(M)$ allora (M_i) è una serie di composizione, perché altrimenti — per definizione di serie di composizione come catena massimale — potremmo estenderla a una catena troppo lunga. Sempre per definizione una catena di lunghezza minore di $\ell(M)$, che quindi non è massimale, può essere estesa fino a diventare una serie di composizione. □

Quali sono, dunque, i moduli "belli", cioè che ammettono una serie di composizione?

Teorema 3.10. *M possiede una serie di composizione se e solo se è sia noetheriano che artiniano.*

Dimostrazione.

"⇒" Se M ha una serie di composizione ogni catena ha lunghezza finita per il Teorema precedente, e non c'è modo di violare né la d.c.c. né la a.c.c.

"⇐" Costruiamo una serie di composizione partendo dall'insieme di tutti i sottomoduli propri di M ed estraendone per noetherianità un elemento massimale M_1. Se $M_1 = 0$ abbiamo finito, altrimenti scegliamo un massimale M_2 fra i sottomoduli propri di M_1. Per artinianità a un certo punto deve valere $M_k = 0$. □

[8] Nel senso di "pezzi", non nel senso algebrico.

Definizione 3.11. In tal caso M si dice *di lunghezza finita*.

Ricordiamo che

Teorema 3.12. Un modulo finitamente generato su un anello artiniano (risp. noetheriano) è artiniano (risp. noetheriano).

Esempio 3.13. Dato che per gli anelli artiniano implica noetheriano, i moduli finitamente generati su un anello artiniano hanno lunghezza finita.

Proposizione 3.14. Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} K \to 0$ una successione esatta di moduli che ammettono serie di composizione[9]. Allora $\ell(N) = \ell(M) + \ell(K)$.

Dimostrazione. Siano $K = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_m$ una serie di composizione per K e $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n$ una per M. Incolliamole come segue:

$$g^{-1}(K_0) \supsetneq \cdots \supsetneq g^{-1}(K_m) = \underbrace{g^{-1}(0) = f(M)}_{\text{esattezza al centro}} = f(M_0) \supsetneq \cdots \supsetneq f(M_n)$$

Questa è massimale perché allungare la parte destra andrebbe contro il fatto che (M_i) è una serie di composizione perché f è iniettiva (cioè per l'esattezza a sinistra), e allungare la parte sinistra contro il fatto che lo è (K_i) per la nota corrispondenza fra sottomoduli nei quozienti (dove stiamo usando l'esattezza a destra). □

Definizione 3.15. Diciamo che due serie di composizione

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_k = 0$$
$$M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_\ell = 0$$

sono *equivalenti* se $k = \ell$ ed esiste una permutazione σ tale che per ogni i si abbia $M_i/M_{i+1} \cong N_{\sigma(i)}/N_{\sigma(i)+1}$.

Ovviamente quella appena definita è una relazione di equivalenza.

Teorema 3.16 (Jordan-Hölder)**.** Due serie di composizione di uno stesso modulo M sono sempre equivalenti.

Dimostrazione. Mostriamo che se l'enunciato è vero per ogni sottomodulo proprio di M allora è vero anche per M. Se M non ha sottomoduli propri l'enunciato è vero a vuoto, e se $M_1 = N_1$ è ovvio[10]. Se non siamo in nessuno di questi due casi allora deve essere $M_1 + N_1 = M$, da cui seguono

$$M\!\diagup_{M_1} \cong N_1\!\diagup_{M_1 \cap N_1} \qquad M\!\diagup_{N_1} \cong M_1\!\diagup_{M_1 \cap N_1}$$

[9] Le ipotesi sono leggermente ridondanti: come corollario della Proposizione, se M e K ammettono serie di composizione anche N ne ammette una.

[10] Se l'enunciato è vero per tutti i sottomoduli allora lo è anche per $M_1 = N_1$, e induttivamente...

Dunque, se $K_1 \supseteq \ldots \supseteq K_s = 0$ è di composizione per $M_1 \cap N_1$, le serie

$$M = M_0 \supseteq M_1 \supseteq M_1 \cap N_1 \supseteq K_1 \supseteq \ldots \supseteq K_s = 0$$
$$M = N_0 \supseteq N_1 \supseteq N_1 \cap M_1 \supseteq K_1 \supseteq \ldots \supseteq K_s = 0$$

sono equivalenti, e per ipotesi induttiva la prima è equivalente a

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_k = 0$$

e la seconda a

$$M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_\ell = 0$$

e per transitività abbiamo finito. □

3.3 Anelli e Moduli Graduati

Definizione 3.17. Un *anello graduato* è un gruppo abeliano della forma

$$A = \bigoplus_{n=0}^{\infty} A_n \qquad A_n \text{ gruppi abeliani}$$

munito di prodotto che, oltre a soddisfare gli assiomi di anello, si comporta bene con la gradazione, cioè $A_i A_j \subseteq A_{i+j}$.

Osservazione 3.18. A_0 è un sottoanello, gli altri A_n sono solo sottogruppi[11].

L'idea che c'è dietro è quella di "scimmiottare" gli anelli di polinomi, dove gli A_j sono i polinomi omogenei di grado esattamente j più lo 0. La nomenclatura continua a seguire questo "esempio madre":

Definizione 3.19. Un elemento non nullo di un anello graduato $A = \bigoplus_{n=0}^{\infty} A_n$ si dice *omogeneo di grado j* se appartiene ad A_j. Per convenzione, il grado di 0 è -1 e si pone $A_{-1} = (0)$.

Definizione 3.20. Se A è un anello graduato, un *A-modulo graduato* è un A-modulo che si scrive come somma diretta di gruppi abeliani

$$M = \bigoplus_{n=0}^{+\infty} M_n$$

dove A agisce in maniera coerente col grado, cioè

$$\underbrace{r_i}_{\in A_i} \cdot \underbrace{m_j}_{\in M_j} \in M_{i+j}$$

[11] Infatti la somma diretta è come gruppi abeliani, non come anelli! Guardare bene la richiesta sulla gradazione.

Osservazione 3.21. Ogni M_n è un A_0-modulo.

Proposizione 3.22. Sia $A = \bigoplus_{n=0}^{\infty} A_n$ un anello graduato noetheriano. Allora A è generato come A_0-algebra da opportuni $x_1, \ldots, x_s$ omogenei di grado $k_1, \ldots, k_s$, con i $k_i > 0$.

Dimostrazione. L'ideale $\bigoplus_{n=1}^{\infty} A_n$ è finitamente generato[12] per noetherianità da $x_1, \ldots, x_s$, che possiamo supporre omogenei[13]. Definiamo la A_0-algebra $A' = A_0[x_1, \ldots, x_s]$ e verifichiamo che $A' = A$ mostrando per induzione su n che ogni A_n è incluso in A'.

Per $n = 0$ è ovvio. Supponiamo che A_r sia incluso in A' per ogni $r < n$ e sia $y \in A_n$. Dato che y appartiene all'ideale $\bigoplus_{m=1}^{\infty} A_m$, possiamo scrivere per ipotesi

$$y = \sum_{i=1}^{s} a_i x_i \qquad a_i \in A$$

Poiché y è omogeneo di grado n e gli x_i sono omogenei di grado k_i dall'espressione sopra se ne può ricavare una simile in cui ogni a_i sia omogeneo di grado $n - k_i$, cioè $a_i \in A_{n-k_i}$: infatti, tutti gli elementi omogenei della somma di grado diverso da n devono cancellarsi, perché y è omogeneo di grado n. Per ipotesi induttiva allora, $a_i \in A_0[x_1, \ldots, x_s]$, e quindi anche $y \in A_0[x_1, \ldots, x_s]$. □

Osservazione 3.23. A è noetheriano se e solo se A_0 lo è e $A = A_0[x_1, \ldots, x_s]$.

Dimostrazione. Una freccia è la Proposizione precedente e il fatto che A_0 si scrive come $A/\bigoplus_{n=1}^{\infty} A_n$. D'altra parte se A_0 è noetheriano possiamo invocare il Teorema della Base di Hilbert. □

Sia A un anello graduato noetheriano e $M = \bigoplus_{n=0}^{\infty} M_n$ un A-modulo graduato finitamente generato. A meno di spezzare in componenti omogenee, M è generato da un numero finito di elementi omogenei $m_1, \ldots, m_t$ di grado $\deg m_j = r_j$. Inoltre anche in questo caso possiamo scrivere ogni $x \in M_n$ come $\sum f_j(x) m_j$ scegliendo $f_j(x)$ è omogeneo di grado $n - r_j$, sostanzialmente riutilizzando lo stesso trucco che abbiamo usato per gli anelli, cioè osservando che i pezzi di grado "sbagliato" si devono cancellare. Di conseguenza abbiamo

Osservazione 3.24. M_n è finitamente generato come A_0-modulo da elementi della forma $g_j(x)m_j$, con g_j un monomio di grado $n - r_j$ nei generatori $x_1, \ldots, x_s$ della Proposizione precedente. In particolare se A_0 è artiniano è ben definita la lunghezza di M_n come A_0-modulo[14].

Un anello graduato che sarà importante più avanti è il seguente:

[12] Come ideale, cioè come A-sottomodulo.
[13] A meno di spezzare in componenti omogenee.
[14] Vedi Esempio 3.13.

Definizione 3.25. Se I è un ideale di A definiamo il *graduato associato ad* I come

$$\operatorname{gr}_I A = \bigoplus_{n=0}^{\infty} {I^n}\big/{I^{n+1}} = {A}\big/{I} \oplus {I}\big/{I^2} \oplus {I^2}\big/{I^3} \oplus \dots$$

Come dovrebbe essere chiaro dalla grafia, gli elementi omogenei di grado n sono quelli di I^n/I^{n+1}.

Un anello A e un suo graduato associato $\operatorname{gr}_I A$ possono somigliarsi molto poco. Ad esempio A può essere un dominio e $\operatorname{gr}_I A$ non esserlo, o viceversa: si veda l'Esercizio A.9. Sotto ipotesi aggiuntive però qualche relazione c'è: si veda la Proposizione 5.26. Esploreremo in dettaglio le relazioni fra un anello noetheriano locale e alcuni suoi graduati associati nel Capitolo 5.

3.4 Serie di Poincaré

La Proposizione 3.14 può essere riformulata dicendo che la lunghezza è una *funzione additiva*:

Definizione 3.26. Sia C una classe di A-moduli e sia G un gruppo abeliano. Una funzione[15] $\lambda\colon C \to G$ viene detta *additiva* se per ogni successione esatta corta

$$0 \to N \to M \to P \to 0$$

vale $\lambda(N) - \lambda(M) + \lambda(P) = 0$.

Esercizio 3.27. Sia λ una funzione additiva e sia

$$0 \to M_n \to \cdots \to M_0 \to 0$$

una successione esatta. Allora

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Hint. Spezzare in esatte corte

$$\begin{array}{ccccccccccc} & & \dots & & \dots & & & & & & \\ & & \searrow & & \nearrow & & & & & & \\ 0 & \to & M_0 & \to & M_1 & \to & \cdots & \to & M_n & \to & 0 \\ & & & \searrow & \nearrow & & & & & & \\ & & & & \operatorname{Im}(\dots) = \operatorname{Ker}(\dots) & & & & & & \\ & & & \nearrow & & \searrow & & & & & \\ & & 0 & & & & 0 & & & & \end{array}$$

[15] A voler essere pignoli forse dovremmo dire qualcosa come "funzione-classe", visto che abbiamo permesso al suo dominio di non essere un insieme. Comunque continueremo ad abusare il linguaggio e a chiamarla "funzione".

□

Definizione 3.28. Siano $M = \bigoplus_{n=0}^{\infty} M_n$ un A-modulo graduato finitamente generato, con A noetheriano, e

$$\lambda\colon \{A_0\text{-moduli finitamente generati}\} \to \mathbb{Z}$$

una funzione additiva. La *serie di Poincaré di M rispetto a λ* è la serie formale

$$P(M,t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n \in \mathbb{Z}[[t]]$$

Per un esempio di calcolo di alcune serie di Poincaré si veda l'Esercizio A.7. Quando la funzione λ è la lunghezza ℓ si parla anche di *serie di Hilbert*.

Teorema 3.29 (Hilbert-Serre)**.** $P(M,t)$ è una funzione razionale della forma

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$$

dove $f(t) \in \mathbb{Z}[t]$, s è il numero di generatori di $A = A_0[x_1, \dots, x_s]$ come A_0-algebra e $k_i = \deg x_i$.

Dimostrazione. La dimostrazione procede per induzione su s. Per $s = 0$ abbiamo $A = A_0$, ed M è un A_0-modulo finitamente generato da $y_1, \dots, y_r$. Sia N il massimo dei gradi di $y_1, \dots, y_r$. Allora per ogni $n > N$ si ha[16] $M_n = 0$, per cui $P(M,t)$ è un polinomio.

Per il passo induttivo scriviamo $A = A_0[x_1, \dots, x_s]$ e consideriamo, per ogni $n \in \mathbb{N}$, l'omomorfismo di A_0-moduli "moltiplicazione per x_s"

$$M_n \xrightarrow{x_s \cdot} M_{n+k_s}$$

e la successione esatta da lui indotta

$$0 \to \underbrace{\operatorname{Ker}(x_s\cdot)}_{=K_n} \to M_n \xrightarrow{x_s\cdot} M_{n+k_s} \to \underbrace{M_{n+k_s}/\operatorname{Im}(x_s\cdot)}_{=L_{n+k_s}} \to 0$$

Poniamo $K = \bigoplus_{n=0}^{\infty} K_n$ e $L = \bigoplus_{n=0}^{\infty} L_n$, e notiamo che sono A-moduli finitamente generati perché K è un sottomodulo di M ed L è un quoziente di M. Non solo: dato che x_s annulla sia K che L questi sono finitamente generati anche come $A_0[x_1, \dots, x_{s-1}]$-moduli, per cui su K ed L possiamo applicare l'ipotesi induttiva (lo faremo tra poco). Applichiamo λ alla successione esatta sopra ottenendo, per l'Esercizio 3.27,

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$$

[16] L'azione di A_0 non aumenta il grado dei generatori; moralmente stiamo moltiplicando per delle costanti.

Moltiplicando per t^{n+k_s} otteniamo

$$t^{n+k_s}\lambda(K_n) - t^{n+k_s}\lambda(M_n) + t^{n+k_s}\lambda(M_{n+k_s}) - t^{n+k_s}\lambda(L_{n+k_s}) = 0$$

e, sommando su tutti gli $n \in \mathbb{N}$,

$$t^{k_s}P(K,t) - t^{k_s}P(M,t) + P(M,t) - \sum_{n=0}^{k_s-1}\lambda(M_n) - P(L,t) + \sum_{n=0}^{k_s-1}\lambda(L_n) = 0$$

Dove quelle somme sono quello che avanza dallo "shift" provocato dalla moltiplicazione per x_s. Facciamo un po' di pulizia: riordiniamo i termini e raccogliamo tutti gli "avanzi" in un polinomio $g(t)$, ottenendo

$$(1-t^{k_s})P(M,t) = -t^{k_s}P(K,t) + P(L,t) + g(t)$$

Usando ora l'ipotesi induttiva su K ed L abbiamo

$$(1-t^{k_s})P(M,t) = -t^{k_s}\frac{p(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})} + \frac{h(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})} + g(t)$$

da cui, dividendo per $(1-t^{k_s})$, si ottiene immediatamente la tesi. □

Corollario 3.30. Nelle notazioni usate finora[17], se i gradi k_i sono tutti 1 allora per n sufficientemente grande $\lambda(M_n)$ risulta un polinomio in n a coefficienti in $\mathbb{Q}$ di grado uguale a $d-1$, dove d è l'ordine del polo di $P(M,t)$ in $t=1$, e in particolare questo grado è $\leq s-1$.

Dimostrazione. Per Teorema di Hilbert-Serre, $\lambda(M_n)$ è il coefficiente di t^n in $f(t)/(1-t)^s = P(M,t)$. Se l'ordine del polo è 0 allora $P(M,t) = f(t)$ è un polinomio e quindi $\lambda(M_n)$ è definitivamente 0, che ha grado -1.

Supponiamo quindi $P(M,t) = f(t)/(1-t)^d$, dove d è l'ordine del polo e $f(1) \neq 0$. Sia $f(t) = \sum_{k=0}^{N} a_k t^k$; sappiamo che vale lo sviluppo in serie

$$\frac{1}{(1-t)^d} = \sum_{k=0}^{\infty}\binom{d+k-1}{d-1}t^k$$

Sostituendo nella formula per $P(M,t)$, otteniamo che il termine di grado n nella serie di potenze viene dato dalla formula[18]

$$\lambda(M_n)t^n = \sum_{k=0}^{\min\{N,n\}} a_k\binom{d+n-k-1}{d-1}t^n$$

[17] Cioè $A = A_0[x_1,\dots,x_s]$ anello graduato noetheriano, k_i grado di x_i, M un A-modulo graduato finitamente generato. Il fatto che A_0 sia artiniano serve per la buona definizione della lunghezza, ma qui λ non è necessariamente la lunghezza ed è data per ipotesi.

[18] Che sembra un sacco spaventosa, ma basta ricordare come si moltiplicano due serie formali.

Supponiamo allora $n \geq N$; pensando a come sono fatti i binomiali ci si accorge subito che il coefficiente di t^n è un polinomio in n di grado al più $d-1$. Effettivamente il grado è proprio $d-1$, e non meno, perché il suo termine di grado massimo è

$$\underbrace{\left(\sum_{k=0}^{N} a_k\right)}_{=f(1)\neq 0} \frac{n^{d-1}}{(d-1)!} \qquad \square$$

Questa Proposizione è un tecnicismo che servirà più avanti:

Proposizione 3.31. Supponiamo che

1. $P(M,t) \neq 0$,
2. $\operatorname{OP}(M) \geq 1$ sia l'ordine del suo polo in 1,
3. $x \in A_k$ non annulla nessun elemento di M,
4. $P(M/xM,t) \neq 0$
5. se $\operatorname{OP}(M) = 1$ allora $\operatorname{OP}(M/xM) \geq 0$.

Allora $\operatorname{OP}(M/xM) = \operatorname{OP}(M) - 1$.

Nota dell'autore[19]: l'ipotesi 5 non segue dalla 4: si potrebbe avere $P(M/xM,t) \neq 0$ ma $P(M/xM,1) = 0$, ad esempio se $P(M/xM,t) = (1-t)^w$ per un qualche w (stiamo considerando gli zeri di ordine k come poli di ordine $-k$).

Dimostrazione. Prendiamo la successione esatta

$$0 \to \underbrace{\operatorname{Ker}(x\cdot)}_{=K_n} \to M_n \xrightarrow{x\cdot} M_{n+k} \to \underbrace{M_{n+k}/\operatorname{Im}(x\cdot)}_{=L_{n+k}} \to 0$$

Dato che x non annulla elementi di M si ha $K_n = (0)$, e quindi $P(K,t) = 0$. Rifacendo lo stesso ragionamento della dimostrazione del Teorema di Hilbert-Serre otteniamo

$$(1-t^k)P(M,t) = -t^k P(K,t) + P(L,t) + g(t) = P(L,t) + g(t)$$

da cui segue la tesi notando che $(1-t)$ ha molteplicità 1 in $(1-t^k)$. $\square$

Tutto ciò tornerà in gioco quando parleremo di Teoria della Dimensione:

[19] L'osservazione forse è banale, ma io personalmente mi sono chiesto per un po' se l'ipotesi 5 fosse superflua, per cui ho pensato che scrivere esplicitamente che non lo è potesse risparmiare qualche grattacapo al lettore.

Spoiler 3.32. Sia A un anello locale noetheriano e $\mathfrak{m}$ un suo ideale massimale. Definiamo anello graduato associato ad A rispetto ad $\mathfrak{m}$

$$\operatorname{gr}_{\mathfrak{m}} A = {}^{A}\!/_{\mathfrak{m}} \oplus {}^{\mathfrak{m}}\!/_{\mathfrak{m}^2} \oplus {}^{\mathfrak{m}^2}\!/_{\mathfrak{m}^3} \oplus \dots$$

e consideriamolo come modulo su se stesso ribattezzandolo M, dove $M_i = \mathfrak{m}^{i-1}/\mathfrak{m}^i$. Inoltre $M_0 = A/\mathfrak{m}$ è un campo e quindi $\ell(M_i) = \dim_{A/\mathfrak{m}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i)$. Si applica allora il Corollario e $\ell(M_i) = \dim_{A/\mathfrak{m}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i)$ è definitivamente un polinomio P. Vedremo che $\dim_{\text{Krull}} A = \deg P + 1$.

Capitolo 4

Completamenti

Questo capitolo ci fornirà dei risultati utili in Teoria della Dimensione, ma è interessante anche per conto suo.

4.1 Definizioni ed Esempi

Definizione 4.1. Un *sistema inverso* è una successione[1] di moduli $\{A_i\}$ equipaggiata con, per ogni $j \geq i$, mappe $\vartheta_{j,i}\colon A_j \to A_i$ tali che ogni $\vartheta_{j,j}$ sia l'identità e che $\vartheta_{j,i} \circ \vartheta_{k,j} = \vartheta_{k,i}$. Il *limite inverso* del sistema[2] $\{A_i\}$ è il modulo

$$\varprojlim A_i = \left\{ a = (a_1, a_2, \ldots, a_n, \ldots) \in \prod A_i \;\middle|\; \forall j > i \; a_i = \vartheta_{j,i}(a_j) \right\}$$

Definizione 4.2. Sia R un gruppo abeliano con una filtrazione, cioè una successione di sottogruppi

$$R = m_0 \supseteq m_1 \supseteq m_2 \supseteq \ldots \supseteq m_n \supseteq \ldots$$

Il *completamento* $\hat{R}$ di R rispetto a $m_0 \supseteq m_1 \supseteq \ldots$ è il limite inverso

$$\hat{R} = \varprojlim {}^{R}\!/_{m_i} = \left\{ g = (g_1, g_2, \ldots, g_n, \ldots) \in \prod R/m_i \;\middle|\; \forall j > i \; g_j \equiv g_i \; (m_i) \right\}$$

Le congruenze modulo m_i sono da intendersi indotte dalla mappa *surgettiva* $\varphi_{j,i}\colon R/m_j \twoheadrightarrow R/m_i$: quello che stiamo chiedendo è quindi che valga $\varphi_{j,i}(g_j) = g_i$.

Osservazione 4.3. Se R è un anello, la filtrazione si intende di ideali e dunque $\hat{R}$ ha una naturale struttura di anello data dal limite inverso.

[1] Non è la definizione più generale possibile, comunque per i nostri scopi basterà.

[2] La notazione "nasconde" le mappe. Questa è prassi comune in letteratura e quindi adotteremo anche noi questa convenzione.

Notazione 4.4. Sia R un anello e I un ideale. Consideriamo la filtrazione

$$R = I^0 \supseteq I \supseteq I^2 \supseteq \dots$$

cioè data da $m_i = I^i$. Il completamento di R rispetto a tale filtrazione è denotato con $\hat{R}_I$.

Esempio 4.5. Chi è il completamento dell'anello $R = S[x_1, \dots, x_n]$ rispetto all'ideale $\mathfrak{m} = (x_1, \dots, x_n)$?

Un elemento di $\hat{R}_\mathfrak{m}$ è della forma $(g_1, g_2, \dots, g_n, \dots)$, dove $g_1 \in R/\mathfrak{m} \cong S$. Invece g_2 è un elemento della forma[3] $[a_0 + a_1 x] \pmod{\mathfrak{m}^2}$. La condizione di compatibilità dice che g_1 è $[a_0] \pmod{\mathfrak{m}}$, e analogamente $g_3 = [a_0 + a_1 x + a_2 x^2] \pmod{\mathfrak{m}^3}$, $g_4 = [a_0 + a_1 x + a_2 x^2 + a_3 x^3] \pmod{\mathfrak{m}^4}$, eccetera. È immediato a questo punto mostrare che

Proposizione 4.6. $\hat{R}_\mathfrak{m} \cong S[[x_1, \dots, x_n]]$, l'anello delle serie formali in n variabili a coefficienti in S.

Esempio 4.7. Sia $p \in \mathbb{Z}$ un primo. Ponendo $I = (p)$ otteniamo l'anello degli *interi p-adici* $\widehat{\mathbb{Z}}_{(p)}$.

Dunque avremo $g_1 \in \mathbb{Z}/p\mathbb{Z}$, $g_2 \in \mathbb{Z}/p^2\mathbb{Z}$, eccetera, ad esempio

$$a = ([1]_5, [11]_{25}, [86]_{125}, [336]_{5^4}, \dots,)$$

Un'altra notazione possibile è

$$a = 1 + 2 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^3 + \dots$$

Per vedere come funzionano le operazioni scriviamone un altro

$$b = ([0]_5, [5]_{25}, [55]_{125}, [305]_{5^4}, \dots,) = 0 + 1 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \dots$$

Sommandoli otteniamo

$$a + b = ([1]_5, [16]_{25}, [16]_{125}, [16]_{5^4} + \dots) = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 0 \cdot 5^3 + (\text{riporto } 1)$$

La differenza sostanziale è che con la prima notazione non c'è bisogno di riporti, con la seconda sì. Il prodotto di due elementi scritti nella seconda forma funziona quasi come per le serie formali[4], tranne per il fatto che bisogna fare i riporti.

Esercizio 4.8. Verificare che in $\widehat{\mathbb{Z}}_{(2)}$ si ha $1 + 2 + 4 + 8 + \dots = -1$, dove $-1 = ([-1], [-1], [-1], \dots)$.

[3] Qui si intende che a_1 e x sono "vettori", nel senso che $a_1 x = a_{1,1} x_1 + \dots, + a_{1,n} x_n$. Analogamente in x^2 ci sono tutti i doppi prodotti delle x_i eccetera.

[4] È veramente più facile capirlo scrivendolo che leggendolo, per cui evito di scriverlo esplicitamente, ma se proprio non vi viene in mente cercate "Prodotto di Cauchy".

Esercizio 4.9. $\widehat{\mathbb{Z}}_{(10)}$ non è un dominio perché si scrive come $\widehat{\mathbb{Z}}_{(2)} \oplus \widehat{\mathbb{Z}}_{(5)}$.

Soluzione. TCR! Basta mandare $([b_i]_{10^i})$ in $\big(([b_i]_{2^i}), ([b_i]_{5^i})\big)$. Questa mappa è un omomorfismo perché data da due proiezioni, è iniettiva per il TCR e surgettiva per lo stesso motivo. □

Battezzando la mappa di prima γ ci possiamo chiedere chi è il w tale che $\gamma(w) = (0, 1)$. Guardando le proiezioni ci accorgiamo subito che deve valere $w_1 \equiv 0 \pmod 2$ e $w_1 \equiv 1 \pmod 5$, e in generale $w_i \equiv 0 \pmod{2^i}$ e $w_i \equiv 1 \pmod{5^i}$.

Esercizio 4.10. Scrivere w in una qualche forma compatta.

Soluzione. È facile vedere che $[w_1]_{10} = [6]_{10}$. Via binomio di Newton uno si accorge che, ad esempio, $6^5 = (1 + 5)^5$ va bene come w_2. Analogamente w_3 può essere rappresentato da $(6^5)^5$, sempre via binomio di Newton. In generale prendere $w_i = 6^{5^{i-1}}$ funziona. □

4.2 Topologia

Sia[5] I un ideale di R e consideriamo gli $r + I^i$ come base di aperti di una topologia su R, dove pensiamo $r + I^i$ come intorni di r. Le mappe $+$ e $\cdot$ risultano continue rispetto a questa topologia, che chiamiamo *I-adica* o *I-topologia*. Possiamo dare una nozione topologica di completamento tramite le successioni di Cauchy:

Definizione 4.11. Una *successione di Cauchy* $\{x_n\}$ in R è una successione tale che per ogni I^j definitivamente $x_\mu - x_\nu \in I^j$. Due successioni di Cauchy $\{x_n\}$ e $\{y_n\}$ sono equivalenti se $\lim_{n\to\infty}(x_n - y_n) = 0$.

Il limite è chiaramente da considerarsi nel senso topologico: per ogni intorno I^j di 0, definitivamente $x_n - y_n \in I^j$. Consideriamo il "completamento topologico" $\tilde{R}$ ottenuto quozientando le successioni di Cauchy modulo equivalenza (esattamente come nella costruzione di $\mathbb{R}$). Dato che le successioni si possono sommare e moltiplicare termine a termine[6], $\tilde{R}$ può essere munito di una struttura di anello. La cosa interessante è che

Teorema 4.12. Gli anelli $\hat{R}$ e $\tilde{R}$ sono isomorfi.

[5] Molte cose funzionerebbero anche con una filtrazione qualsiasi, ma il caso che ci interessa è quello con $m_i = I^i$ e quindi enunciamo quasi tutto in questo caso. Ogni tanto useremo comunque la notazione m_i.

[6] Ad essere onesti bisognerebbe mettersi a verificare che passando al quoziente continua a funzionare tutto, cioè che addizione e moltiplicazione sono bene definite anche sul quoziente, ma si spera che il lettore sia in grado di curare questi dettagli per conto suo.

Dimostrazione. Dove mandiamo una successione di Cauchy $\{x_n\}$? Dire che definitivamente $x_\mu - x_\nu \in m_j$ vuol dire che la proiezione di x_n su R/m_j è definitivamente costante, e questo sarà il nostro g_j. È chiaro che questo non dipende dalla scelta del rappresentante per $\{x_n\}$. L'iniettività è una diretta conseguenza delle definizioni e per la surgettività basta notare che $(g_1, g_2, \ldots, g_n, \ldots)$ è raggiunto da $\{g_i\}$. □

Completare rispetto ad un massimale ha il simpatico effetto "collaterale" di produrre un anello locale:

Proposizione 4.13. Sia $\mathfrak{m} \in \operatorname{SpecMax}(R)$. Allora $\hat{R}_\mathfrak{m}$ è un anello locale con ideale massimale $\hat{\mathfrak{m}} = \{(g_1, \ldots, g_n, \ldots) \mid g_1 = 0\}$.

Dimostrazione. Sia $g = (g_1, \ldots, g_n, \ldots) \in \hat{R}_\mathfrak{m} \setminus \hat{\mathfrak{m}}$, cioè con $g_1 \neq [0]$. Dunque per la condizione di compatibilità $g_2 \notin \mathfrak{m}R/\mathfrak{m}^2$. Dato che questo è l'unico massimale dell'anello locale $R/\mathfrak{m}^2$, g_2 è invertibile. Allo stesso modo si mostra che g_j è invertibile in $R/\mathfrak{m}^j$. Dato che $g_1 \in R/\mathfrak{m}$ è non nullo in un campo è anche lui invertibile, e quindi l'inverso di g è

$$h = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}, \ldots)$$

a patto di mostrare che valga la compatibilità fra le coordinate, cioè che $g_i \varphi_{j,i}(g_j^{-1}) \equiv 1 \pmod{\mathfrak{m}^i}$; ma questo è vero perché $\varphi_{j,i}(g_j)\varphi_{j,i}(g_j^{-1}) \equiv 1 \pmod{\mathfrak{m}^i}$. Viceversa, se $g_1 = 0$, è palese per com'è fatto il prodotto nel completamento che g non può avere un inverso. □

Proposizione 4.14. La topologia I-adica su R è di Hausdorff se e solo se $\bigcap I^j = \{0\}$, ovvero se e solo se $R \to \hat{R}_I$ è iniettiva.

Dimostrazione. Preliminarmente studiamo la chiusura dello 0. Usando la definizione di chiusura con i punti di aderenza abbiamo $a \in \overline{\{0\}}$ se e solo se per ogni j si ha $0 \in a + I^j$, cioè $-a \in I^j$, o equivalentemente, dato che I^j è un ideale e in particolare un sottogruppo, $a \in \bigcap I^j$. Dunque $\overline{\{0\}} = \bigcap I^j$.

Quindi se $\bigcap I^j = \{0\}$ allora $\{0\}$ è chiuso[7], e $\Delta = \{(x, x) \in R \times R\}$ è chiusa in $R \times R$ perché è la controimmagine di 0 secondo la somma, che è continua, ma avere la diagonale chiusa nel prodotto è equivalente ad essere di Hausdorff[8]. Viceversa se R è di Hausdorff tutti i punti sono chiusi, e in particolare lo è $\{0\}$.

Per l'ultima parte della tesi basta notare che il nucleo della mappa $\vartheta\colon R \to \hat{R}_I$ che manda r in $([r]_I, [r]_{I^2}, \ldots, [r]_{I^n}, \ldots)$ è proprio $\bigcap I^j$. □

[7] E similmente lo sono tutti i punti, perché le traslazioni sono continue.

[8] Qui uno potrebbe rimanere sdubbiato, dato che avere i punti chiusi è più debole che essere di Hausdorff. Il punto è che il "lavoro sporco" lo fa la continuità della somma o, in altre parole, l'ipotesi in più è quella di trovarsi in un gruppo topologico.

Definizione 4.15. Siano R un anello e I un suo ideale. Diciamo che R è completo rispetto alla topologia I-adica se la mappa $R \to \hat{R}_I$ è un isomorfismo.

Per l'iniettività deve essere, per quanto appena visto, $\bigcap I^j = 0$. Comunque detta in altro modo vuol dire che le successioni di Cauchy convergono. Come ci si aspetta, i completamenti di qualcos'altro *sono* completi. Più precisamente

Proposizione 4.16. Siano in $\hat{R}_I$ gli ideali $\hat{I}_n$ dati dalle liste che iniziano con n zeri. Allora

$$\widehat{\left(\hat{R}_I\right)}_{\{\hat{I}_n\}} \cong \hat{R}_I$$

Teorema 4.17 (di Intersezione di Krull)**.** Siano I un ideale di un anello R noetheriano ed M un R-modulo finitamente generato. Allora esiste $r \in I$ tale che $(1+r)(\bigcap_j I^j M) = \{0\}$.

Corollario 4.18. Se M coincide con R, e questo è un dominio oppure è locale, e I è proprio allora $\bigcap_j I^j = \{0\}$.

Dimostrazione. Se R è un dominio ed esiste $a \neq 0 \in (\bigcap_j I^j M)$ tale che $(1+r)a = 0$ allora $r = -1 \in I$. Se invece R è locale $1 + r$ non può stare nell'unico massimale perché sennò ci starebbe 1, e quindi è invertibile. □

Corollario 4.19. Se R è un dominio noetheriano o un anello noetheriano locale e I è proprio, la topologia I-adica è di Hausdorff.

La dimostrazione del Teorema di Intersezione di Krull passa da un risultato importante che sarà anche utile in seguito, e cui è non a caso dedicata tutta la prossima sezione, ma il caso $R = M$ può essere dimostrato in maniera abbastanza ingegnosa anche direttamente:

Dimostrazione. Facciamo vedere che se $x \in \bigcap I^j$ allora $x \in xI$. Questo basta perché allora $x = xr$, per cui possiamo scrivere $(1-r)x = 0$ e abbiamo

$$\bigcap I^j = \{x \in R \mid \exists r \in I \ (1-r)x = 0\}$$

dove la $\subseteq$ segue da quanto detto e la $\supseteq$ segue scrivendo $x = rx = r^2x = r^3x = \ldots$. Ma siccome R è noetheriano $\bigcap I^j$ è finitamente generato da $x_1, \ldots, x_n$, ognuno col suo $(1-r_i)$ e il prodotto $\prod(1-r_i) = 1 + \tilde{r}$ uccide tutto $\bigcap I^j$.

Supponiamo che $I = (b_1, \ldots, b_r)$. Dato che per ogni n si ha $x \in I^n$ esiste un polinomio di grado n omogeneo[9] $P_n(T_1, \ldots, T_r) \in R[T_1, \ldots, T_r]$ tale che

[9] Basta pensare a chi sono i generatori di I^n.

$x = P_n(b_1, \ldots, b_r)$. Dato che $R[T_1, \ldots, T_r]$ è noetheriano per il Teorema della Base di Hilbert, posto $J_n = (P_1, P_2, \ldots, P_n)$ la catena

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_n \subseteq \ldots$$

si stabilizza da un certo N in poi, e quindi possiamo scrivere

$$P_{N+1} = Q_N P_1 + \ldots + Q_1 P_N$$

dove i Q_i sono omogenei[10] di grado i. A questo punto valutiamo in $(b_1, \ldots, b_r)$ e troviamo

$$x = \big(Q_1(b_1, \ldots, b_r) + \ldots + Q_N(b_1, \ldots, b_r)\big)x$$

ma dato che i Q_i sono omogenei di grado positivo ognuno degli addendi fra parentesi sta in I e questo prova la tesi. □

Rimossa l'ipotesi di noetherianità, in alcuni anelli (vedi Osservazione 4.25) il "Teorema" non funziona, a volte nemmeno per I massimale[11].

4.3 Il Lemma di Artin-Rees

Le filtrazioni ottenute con potenze di un ideale I sono un esempio di *filtrazione moltiplicativa*, cioè che si comporta bene rispetto al prodotto. Precisamente

Definizione 4.20. Una filtrazione

$$R = I_0 \supset I_1 \supset \ldots \supset I_n \supset \ldots$$

con gli I_j ideali si dice *moltiplicativa* se $\forall i, j\ I_j \cdot I_j \subseteq I_{i+j}$.

Definizione 4.21. Sia M un R-modulo e I un ideale. Una filtrazione in sottomoduli

$$M = M_0 \supset M_1 \supset \ldots \supset M_n \supset \ldots$$

è una *I-filtrazione* se si comporta bene rispetto a I, cioè se $\forall n \geq 0\ IM_n \subseteq M_{n+1}$. Se definitivamente vale $IM_n = M_{n+1}$ diciamo che la I-filtrazione è *I-stabile*.

Esempio 4.22 (madre di tutti gli esempi)**.** La filtrazione

$$M \supset IM \supset \ldots \supset I^n M \supset \ldots$$

è I-stabile.

[10] A meno dei soliti trucchi.

[11] L'ideale dell'Osservazione 4.25 *non* è massimale.

Lemma 4.23 (di Artin-Rees)**.** Sia R un anello noetheriano, I un suo ideale e $M' \subset M$ moduli finitamente generati. Se

$$M = M_0 \supset M_1 \supset \ldots \supset M_n \supset \ldots$$

è una filtrazione I-stabile, allora la *filtrazione indotta*

$$M' \supset M' \cap M_1 \supset \ldots \supset M' \cap M_n \supset \ldots$$

è I-stabile.

Dato che questo è uno di quegli enunciati che a prima vista sembrano dire poco, prima di dimostrarlo "facciamolo parlare" usandolo per la

Dimostrazione del Teorema di Intersezione di Krull. Sia $M' = \bigcap_{j\in\mathbb{N}} I^j M$. La filtrazione

$$M \supset IM \supset \ldots \supset I^n M \supset \ldots$$

è I-stabile. Per Artin-Rees dunque anche

$$M' \supset M' \cap IM \supset \ldots \supset M' \cap I^n M \supset \ldots$$

è I-stabile da un certo p in poi, e abbiamo

$$M' = \bigcap_{j\in\mathbb{N}} I^j M = \overbrace{\bigcap_{j\in\mathbb{N}} I^j M \cap I^{p+1} M}^{M'\cap I^{p+1}M} \underbrace{=}_{\text{A.R.}} \overbrace{I\Big(\bigcap_{j\in\mathbb{N}} I^j M \cap I^p M\Big)}^{I(M'\cap I^p M)} = IM'$$

E allora per Nakayama[12] esiste $r \in I$ tale che $(1+r)M' = 0$. □

Qui qualcuno potrebbe gridare all'imbroglio, nel senso che magari si immaginava che in generale valga

$$I\Big(\bigcap_{j\in\mathbb{N}} I^j M\Big) = \bigcap_{j\in\mathbb{N}} I^j M$$

e quindi non ci sarebbe bisogno di Artin-Rees. Peccato che questo sia falso:

Controesempio 4.24. Sia $M = R$ l'anello $\mathbb{Z}[x, y_1, y_2, \ldots]$ quozientato per l'ideale J delle relazioni

$$\begin{aligned} &px = 0 \\ &x = py_1 = p^2 y_2 = \ldots = p^n y_n = \ldots \\ &x^2 = xy_j = y_i y_j = y_i^2 = 0 \end{aligned}$$

Qui, se $I = (p)$, succede che $\bigcap I^j = (x)$, da cui segue

$$I \cdot \Big(\bigcap I^j\Big) = I(x) = (px) = (0) \neq \bigcap I^j$$

[12]Qui "Nakayama" è "Se I è un ideale di A ed M è un A-modulo finitamente generato tale che $IM = M$ allora esiste $r \in I$ tale che $(1+r)M = 0$." Non è necessario che I sia nel Jacobson.

Dimostrazione. Osserviamo subito che $x \in \bigcap I^j$, e quindi $(x) \subseteq \bigcap I^j$, perché per ogni j possiamo scrivere $x = p^j y_j$. Per l'altra inclusione notiamo che $\bigcap I^j \subseteq \langle x, y_1, y_2, \ldots \rangle_{\mathbb{Z}}$, cioè non ci sono costanti, e sia

$$z = \alpha x + \alpha_1 y_1 + \alpha_2 y_2 + \ldots + \alpha_m y_m \in \bigcap I^j$$

Scegliamo $t > m$ e leggiamo $z \in I^t$ in $\mathbb{Z}[x, y_1, y_2, \ldots]$, prima di quozientare:

$$\alpha x + \alpha_1 y_1 + \alpha_2 y_2 + \ldots + \alpha_m y_m + \underbrace{q(x, y_1, \ldots, y_n)}_{\in J} = p^t(\alpha' x + \alpha_1' y_1 + \ldots)$$

Focalizzando l'attenzione[13] su y_1 notiamo che

$$\alpha_1 y_1 + (\underbrace{\ldots}_{\gamma p y_1}) = p^t \alpha_1' y_1$$

dunque $p \mid \alpha_1$, e possiamo riscrivere $\alpha_1 y_1$ in termini di x. La stessa cosa la possiamo fare con le altre variabili, e concludiamo che $\alpha x + \alpha_1 y_1 + \alpha_2 y_2 + \ldots + \alpha_m y_m \in (x)$, da cui l'inclusione $\bigcap I^j \subseteq (x)$. □

Osservazione 4.25. Abbiamo incidentalmente mostrato che le ipotesi di Krull sono necessarie. Infatti nel controesempio precedente comunque scelto $r \in I = (p)$ abbiamo $(1 + r)(x) = (x)$.

Per dimostrare Artin-Rees ci serve qualche altra nozione preliminare:

Definizione 4.26. Dato R anello e I ideale definiamo il *blow up*[14] *di I in R* come l'anello graduato[15]

$$B_I R = R \oplus I \oplus I^2 \oplus \ldots \oplus I^n \oplus \ldots \cong R[tI]$$

Osservazione 4.27. Se M è un R-modulo e J è una I-filtrazione $M_0 \supset \ldots \supset M_n \supset \ldots$ allora

$$B_J M = M \oplus M_1 \oplus \ldots \oplus M_n \oplus \ldots$$

è un $B_I R$-modulo graduato[16].

Proposizione 4.28. Sia R un anello, I un ideale, M un R-modulo finitamente generato e J una filtrazione $M = M_0 \supset \ldots$ data da moduli finitamente generati M_i. Allora la filtrazione J è I-stabile se e solo se $B_J M$ è un $B_I R$-modulo finitamente generato.

[13] Cioè dicendo che i monomi in y_1 a sinistra e a destra devono coincidere.

[14] Sì, viene dalla geometria algebrica. È una costruzione in cui si elimina una sottovarietà e si rimpiazza con il proiettivo del tangente (nel caso in cui la sottovarietà sia un punto)... Per saperne di più si veda la sezione 5.2 di [5].

[15] La notazione $R[tI]$ è mnemonica, per dire che i prodotti vanno letti nell'I_n opportuno.

[16] Basta scrivere le definizioni e pensarci un attimo.

Dimostrazione. Se $B_J M$ è finitamente generato come $B_I R$-modulo i suoi generatori staranno in $\bigoplus_{i=0}^{n} M_i$ per un certo n. Al solito, prendiamo dei generatori omogenei. Consideriamo poi che la parte finale $\bigoplus_{i=n}^{\infty} M_i$ è generata come $B_I R$-modulo dal solo[17] M_n, ovvero $M_{n+i} = I^i M_n$, per cui J è I-stabile. Viceversa se J è I-stabile — diciamo da n in poi — allora $B_J M$ è generato come $B_I R$-modulo dai generatori (finiti per ipotesi) di $M_0, \dots, M_n$. □

Siamo pronti per affrontare la

Dimostrazione del Lemma di Artin-Rees. Battezziamo le filtrazioni J e J', chiamiamo $M'_i = M' \cap M_i$ e notiamo subito che $B_{J'} M'$ è un $B_I R$-sottomodulo graduato di $B_J M$. Dato che J è I-stabile, per la Proposizione precedente $B_J M$ è un $B_I R$-modulo finitamente generato. Ma $B_I R$ è una R-algebra finitamente generata perché R è noetheriano e possiamo pensarla come algebra polinomiale $R[g_1, \dots, g_k]$. Invocando il Teorema della Base di Hilbert sappiamo che $B_I R$ è noetheriano, e siccome un modulo finitamente generato su un anello noetheriano è noetheriano, $B_J M$ è un $B_I R$-modulo noetheriano, e $B'_J M'$ in quanto suo sottomodulo deve essere finitamente generato. Per la Proposizione precedente possiamo allora concludere che J' è I-stabile. □

Il Lemma di Artin-Rees ha anche un significato topologico, che passa dalla seguente

Proposizione 4.29. Se $\{M_n\}$ e $\{\overline{M}_n\}$ sono filtrazioni I-stabili di un modulo M, allora hanno "differenze limitate", cioè esiste n_0 tale che per ogni n vale sia $M_{n+n_0} \subseteq \overline{M}_n$ che $\overline{M}_{n+n_0} \subseteq M_n$. In particolare tutte le filtrazioni I-stabili inducono la stessa topologia su M.

Dimostrazione. Basta confrontare $\{M_n\}$ con la filtrazione $\{I^j M\}$; fatto questo basterà usarla "di passaggio" per confrontare due filtrazioni I-stabili qualunque. Supponiamo che M sia stabile da n_0 in poi. Da un lato, poiché per ogni $n \geq n_0$ vale $IM_n = M_{n+1}$, abbiamo $M_{n+n_0} = I^n M_{n_0} \subset I^n M$. Dall'altro, dato che $IM_n \subseteq M_{n+1}$ per definizione di I-filtrazione, allora $I^n M \subset M_n$ e quindi $I^{n+n_0} M \subset M_{n+n_0} \subset M_n$. □

Teorema 4.30 (Interpretazione Topologica di Artin-Rees)**.** Siano R noetheriano, I un ideale, M un R-modulo finitamente generato e M' un suo sottomodulo. Allora le filtrazioni $\{I^n M'\}$ e $\{I^n M \cap M'\}$ hanno differenze limitate e in particolare la I-topologia di M' coincide con la topologia indotta dalla I-topologia di M.

Proviamo a "rompere" questo risultato togliendo delle ipotesi e vedendo come fallisce. Vogliamo dunque due moduli $M' \subseteq M$ tali che la I-topologia

[17] Ad esempio se $n = 10$ e prendiamo $y \in M_{1000}$ questo verrà da — poniamo — un elemento di M_3 per uno di I^{997}. Comunque moltiplicando 997 volte per elementi di I prima o poi da M_n bisogna passarci.

su M' considerato come modulo a sé stante *non* coincida con la topologia indotta come sottospazio dalla I-topologia di M.

Controesempio 4.31. Siano p primo, $A = \bigoplus_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z}$ e $B = \bigoplus_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Consideriamo l'omomorfismo di $\mathbb{Z}$-moduli $\alpha\colon A \hookrightarrow B$ "che manda 1 in p^{n-1}" e usiamolo per leggere A come sottomodulo di B.

Dato che $pA = 0$, il completamento $\hat{A}_{(p)}$ rispetto alla topologia indotta dall'ideale (p) è

$$\hat{A}_{(p)} = \varprojlim A/p^n A = \varprojlim A \cong A$$

Studiamo ora la topologia (p)-adica di B, ovvero studiamo $\hat{B}_{(p)}$. Abbiamo

$$pB \cong \bigoplus_{n=2}^{\infty} p\mathbb{Z}/p^n\mathbb{Z}$$

e, in generale, per induzione

$$p^k B \cong \bigoplus_{n=k+1}^{\infty} p^k\mathbb{Z}/p^n\mathbb{Z}$$

e questi sono gli intorni di 0. La topologia indotta su A ha come intorni di 0 di base $\alpha(A) \cap p^k B$. Dato che

$$\alpha(A) = \bigoplus_{n=1}^{\infty} p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$$

abbiamo immediatamente

$$\alpha(A) \cap p^k B \cong \bigoplus_{n=k+1}^{\infty} p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$$

e quindi la filtrazione di $\alpha(A) \cong A$ indotta è

$$\alpha(A) = \bigoplus_{n=1}^{\infty} p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \supset \bigoplus_{n=2}^{\infty} p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \supset \bigoplus_{n=3}^{\infty} p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \supset \dots$$

Ne segue che il completamento di A rispetto alla topologia indotta dalla (p)-topologia di B è

$$\varprojlim \frac{\alpha(A)}{\alpha(A) \cap p^k B} = \varprojlim \bigoplus_{n=1}^{k} p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$$

dove la mappa è quella che "dimentica le ultime coordinate", che si vede facilmente essere "compatibile", per cui quello che abbiamo scritto *è* un sistema inverso. Inoltre chiaramente

$$\varprojlim \bigoplus_{n=1}^{k} p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \cong \varprojlim \bigoplus_{n=1}^{k} \mathbb{Z}/p\mathbb{Z} \cong \prod_{i=1}^{\infty} \mathbb{Z}/p\mathbb{Z}$$

dove il secondo isomorfismo segue dal fatto che un elemento del termine centrale deve essere della forma $g(a,(a,b),(a,b,c),\ldots)$. Per concludere basta notare che i due completamenti $A = \bigoplus_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z}$ e $\prod_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z}$ non sono isomorfi, ad esempio per motivi di cardinalità[18], per cui le topologie che li inducono non possono coincidere.

4.4 Completamenti e Successioni Esatte

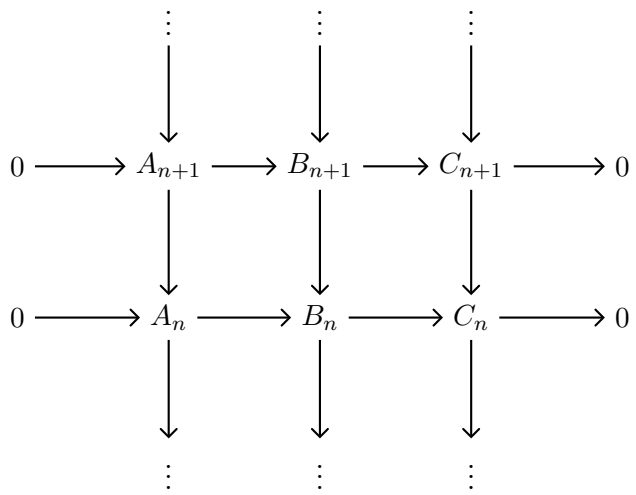
L'obiettivo principale di questa sezione è dimostrare la seguente

Proposizione 4.32. Sia $0 \to M' \to M \to M'' \to 0$ una successione esatta di moduli finitamente generati su un anello noetheriano A. Sia I un ideale di A. Allora è esatta anche[19]

$$0 \to \widehat{M'}_I \to \widehat{M}_I \to \widehat{M''}_I \to 0$$

Per arrivarci ci servono un paio di risultati.

Proposizione 4.33. Sia $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ una successione esatta di sistemi inversi di R-moduli, cioè una famiglia di mappe che faccia commutare tutti i quadrati e renda esatte tutte le righe come in figura



allora è esatta anche

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$$

se inoltre $\{A_n\}$ ha tutte le mappe surgettive è esatta anche

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

[18] Il primo è numerabile in quanto unione numerabile di finiti, il secondo no perché ha cardinalità $p^{\aleph_0} = 2^{\aleph_0} > \aleph_0$.

[19] Dovrebbe essere chiaro chi sono le mappe.

Dimostrazione. Siano $A = \prod A_n$, $B = \prod B_n$ e $C = \prod C_n$. Se le mappe del sistema inverso $\{A_n\}$ sono $\{\vartheta_{n+1}\colon A_{n+1} \to A_n\}$ definiamo $d^A\colon A \to A$ componente su componente come $a_n \mapsto a_n - \vartheta_{n+1}(a_{n+1})$. Definendo analogamente d^B e d^C otteniamo il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

Se applichiamo il Lemma del Serpente troviamo la successione esatta

$$0 \to \operatorname{Ker} d^A \to \operatorname{Ker} d^B \to \operatorname{Ker} d^C \to \operatorname{Coker} d^A \to \operatorname{Coker} d^B \to \operatorname{Coker} d^C \to 0$$

Per la prima parte della tesi basta[20] accorgersi che, per definizione, $\operatorname{Ker} d^A = \varprojlim A_n$, e analogamente per B e C. Per portare a casa la seconda parte della tesi vorremmo mostrare che $\operatorname{Coker} d^A = 0$, cioè che d^A è surgettiva. Ma per avere d^A surgettiva bisogna risolvere dei sistemi della forma

$$\begin{cases} a_1 = d^A(x_1) = x_1 - \vartheta_2(x_2) \\ a_2 = d^A(x_2) = x_2 - \vartheta_3(x_3) \\ \vdots \end{cases}$$

cosa possibile trovando induttivamente x_n per surgettività delle ϑ_n. □

Corollario 4.34. Sia $0 \to M' \to M \xrightarrow{\pi} M'' \to 0$ una successione esatta di R-moduli e muniamo M, M', M'' delle topologie indotte rispettivamente dalle filtrazioni[21] $\{M_n\}$, $\{M_n \cap M'\}$ e $\{\pi(M_n)\}$. Allora è esatta anche la successione $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$.

Dimostrazione. Basta applicare la Proposizione precedente a

$$0 \to \underbrace{\left\{M' \big/ M_n \cap M'\right\}}_{=\{A_n\}} \to \underbrace{\left\{M \big/ M_n\right\}}_{=\{B_n\}} \to \underbrace{\left\{M'' \big/ \pi(M_n)\right\}}_{=\{C_n\}} \to 0$$

dove le ϑ_i sono le proiezioni al quoziente[22], e quindi sono surgettive. □

Ora abbiamo gli strumenti per affrontare la

Dimostrazione della Proposizione 4.32. Al centro c'è la filtrazione $\{I^j M\}$, a destra abbiamo

$$\{I^j M''\} = \{I^j \pi(M)\} = \{\pi(I^j M)\}$$

[20] Le mappe sono le stesse perché quelle del Lemma del Serpente sono le restrizioni.
[21] Nel senso che $\{M_n\}$ è data per ipotesi e le altre due sono indotte da questa.
[22] E anche le mappe per i B_n e i C_n, che non abbiamo mai battezzato.

e a sinistra abbiamo $\{I^j M'\}$, che comunque induce la stessa topologia di $\{I^j M \cap M'\}$ per Artin-Rees. Possiamo dunque applicare il Corollario precedente e concludere. □

Esercizio 4.35. Sia A un anello e I un suo ideale. Sia $x \in A$ non divisore di 0. Consideriamo la mappa $A \to \widehat{A}_I$ che associa $x \mapsto \hat{x}$. Ci chiediamo se $\hat{x}$ può essere un divisore di 0.

Soluzione. Consideriamo

$$0 \to A \xrightarrow{\cdot x} A \to {}^{A}\!/_{xA} \to 0$$

dove $\cdot x$ è iniettiva perché x non è un divisore di 0. Se si passa ai completamenti salta fuori $\widehat{A}_{\{xA \cap I^j\}}$, che in generale potrebbe non coincidere con $\widehat{A}_I$. Se aggiungiamo l'ipotesi che A sia noetheriano, però, tutto funziona perché possiamo usare la[23] Proposizione 4.32 e la mappa $\cdot x$, passando ai completamenti, rimane iniettiva[24]. □

Questo *non* vuol dire che A dominio implichi $\widehat{A}_I$ dominio: nell'Esercizio 4.9 abbiamo già visto che è falso.

4.5 Sollevamento di Hensel

Diciamo di avere fra le mani un certo $F \in \mathbb{Z}[x]$ e di volerlo fattorizzare. Se $F = GH$, con $\deg G = r$, possiamo "predire" in un qualche modo che i coefficienti di G siano minori di un certo M in modulo. Supponiamo di trovare una fattorizzazione $f \equiv gh \pmod{M}$ con g di grado r e — per semplicità — h irriducibile (qui ci sono algoritmi a bizzeffe). Scegliamo un rappresentante di g con i coefficienti in modulo minori di $M/2$. Ora succede che questo rappresentante $g \in \mathbb{Z}[x]$ o divide F oppure F non ha fattori di grado r. Infatti un eventuale $g' \equiv g$ diverso avrebbe alcuni coefficienti che distano troppo da quelli di g. Dunque basta controllare tutte le fattorizzazioni modulo M per vedere se F è irriducibile in $\mathbb{Z}[x]$. Questo si chiama *sollevamento Henseliano*. Queste idee si trasferiscono in anelli completi:

Lemma 4.36 (di Hensel)**.** Sia R un anello locale[25] *completo*, cioè tale che $R \to \widehat{R}_{\mathfrak{m}}$ è un isomorfismo, ovvero in cui tutte le successioni di Cauchy convergono[26]. Siano poi $K = R/\mathfrak{m}$ il suo campo residuo e $F \in R[X]$ un polinomio monico che si fattorizza come[27] $f = gh$ in $K[X]$, cioè $f \equiv gh$

[23] Serve passare dalla Proposizione 4.32, e non basta il Corollario 4.34. Il punto è che nel Corollario abbiamo letto M' direttamente dentro M, nel senso che abbiamo considerato $\{M' \cap i^{-1}(M_n)\}$.

[24] La mappa "passata" sarebbe $\cdot\hat{x}$, dove $\hat{x} = (x, x, x, \ldots)$.

[25] D'ora in poi se un anello è locale il suo ideale massimale si chiamerà $\mathfrak{m}$.

[26] Nella topologia $\mathfrak{m}$-adica.

[27] La convenzione è che le lettere maiuscole vivono in $R[X]$ e le rispettive minuscole sono le classi di resto modulo $\mathfrak{m}$.

(mod $\mathfrak{m}$), dove g e h sono primi fra loro e monici. Allora si può sollevare la fattorizzazione a $F = GH$ in $R[X]$. Tale fattorizzazione è unica.

L'unicità non la dimostreremo.

Dimostrazione dell'Esistenza. Siano G_1 e H_1 monici tali che $g_1 \equiv g \pmod{\mathfrak{m}}$, $h_1 \equiv h \pmod{\mathfrak{m}}$, $\deg G_1 = \deg g_1$ e $\deg H_1 = \deg h_1$. Per opportuni $A_i \in \mathfrak{m}$ e $J_i \in R[X]$ in $R[X]$ vale

$$F - G_1 H_1 = \sum A_i J_i$$

inoltre $\deg J_i < \deg F$ perché i polinomi F e $G_1 H_1$ sono monici e il termine di grado massimo si cancella. Siccome $(g, h) = 1$, per Bézout possiamo scrivere in $K[X]$

$$j_i = g u_i + h v_i$$

dove possiamo supporre che $\deg u_i < \deg h$ a meno di rimpiazzare u_i col suo resto modulo h e buttare l'altro pezzo in h. Allora è facile vedere che[28]

$$\deg(h v_i) = \deg(j_i - g u_i) < \deg f$$

per cui $\deg v_i < \deg g$. Scegliamo U_i e V_i con $\deg U_i = \deg u_i$ e $\deg V_i = \deg v_i$ e definiamo

$$G_2 = G_1 + \sum A_i V_i \qquad H_2 = H_1 + \sum A_i U_i$$

Per poi andare a calcolare

$$F - G_2 H_2 = F - G_1 H_1 - \sum A_i (\underbrace{H_1 V_i + G_1 U_i}_{= J_i + \Gamma_i}) - \sum A_i A_j U_i V_j$$

dove $\Gamma_i \in \mathfrak{m}[X]$, dato che J_i è il sollevato di $j_i = h v_i + g u_i$. Ne deduciamo che quanto sopra è uguale a

$$\underbrace{F - G_1 H_1 - \sum A_i J_i}_{=0} - \sum \underbrace{A_i}_{\in \mathfrak{m}} \underbrace{\Gamma_i}_{\in \mathfrak{m}[X]} - \sum \underbrace{A_i}_{\in \mathfrak{m}} \underbrace{A_j}_{\in \mathfrak{m}} U_i V_j$$

e quindi $F \equiv G_2 H_2 \pmod{\mathfrak{m}^2}$. Ora G_2 e H_2 sono monici perché $\deg V_i < \deg G_1$, $\deg U_i < \deg H_1$ e $\deg A_i = 0$, per cui nella loro definizione non si intaccava il coefficiente direttivo. Analogamente possiamo fare gli altri passi, ottenendo due successioni $\{G_n\}$ e $\{H_n\}$ in $R[X]$ tali che $G_i H_i \equiv F \pmod{\mathfrak{m}^i}$. La successione coefficiente per coefficiente $G_1^k, G_2^k, \ldots$ è di Cauchy e quindi, per la completezza di R, ha un limite G^k, e questo è come costruiamo G e H. Vediamo se vanno bene. Monici lo sono, ma che $GH = F$ è vero? Basta ragionare per intorni come in analisi: fissiamo $\mathfrak{m}^s$. Definitivamente $G_n - G \in \mathfrak{m}^s$ e $H_n - H \in \mathfrak{m}^s$, e a maggior ragione $GH - G_n H_n \in \mathfrak{m}^s$. D'altra parte $F \equiv G_n H_n \pmod{\mathfrak{m}^n}$. Dunque per ogni s si ha $F - GH \in \mathfrak{m}^s$ e per completezza $F - GH = 0$. □

[28] Per il fatto che $\deg f = \deg F$ si usa che F è monico.

Dove abbiamo usato l'ipotesi che R fosse locale? Ovunque e da nessuna parte, nel senso che per la Proposizione 4.13 il completamento di un anello rispetto a un massimale è locale, per cui un anello completo è necessariamente locale.

Esempio 4.37. In $\widehat{\mathbb{Z}}_{(5)}$ prendiamo $F = x^2 + 1$ e ci chiediamo se ha radici.

Ricordandosi chi è l'ideale massimale dei completati[29] si vede subito che

$$\widehat{\mathbb{Z}}_{(5)}\big/_{(5)} \cong \mathbb{Z}\big/_{5\mathbb{Z}} = K$$

Abbiamo, in $(\mathbb{Z}/5\mathbb{Z})[x]$,

$$x^2 + 1 = \underbrace{(x-2)}_{g}\underbrace{(x-3)}_{h}$$

con g, h monici e primi fra loro. Per Hensel esistono G e H monici di grado 1 tali che $x^2 + 1 = GH$. Dunque $G = (x - \alpha)$ e $H = (x - \beta)$, e $\alpha = (2, \ldots)$, e $\beta = (3, \ldots)$ sono le radici cercate.

Esempio 4.38. Consideriamo il completamento di $\mathbb{C}[z]$, cioè $\mathbb{C}[[z]]$, con ideale massimale (z), e guardiamo $F(x) = x^2 - (1 + z)$ in $\mathbb{C}[[z]][x]$.

Il campo residuo in questo caso è $\mathbb{C}$, e in $\mathbb{C}[x]$ abbiamo $f(x) = x^2 - 1 = (x - 1)(x + 1)$. Sollevando troviamo $\alpha(z)$, $\beta(z)$ radici quadrate di $1 + z$ in $\mathbb{C}[[z]]$.

Esercizio 4.39. Sia A completo rispetto ad un ideale massimale $\mathfrak{m}$ (in particolare A è locale). Sia U il sottogruppo $1 + \mathfrak{m}$ del gruppo moltiplicativo A^*. Sia infine n un intero positivo primo con la caratteristica[30] di $A/\mathfrak{m}$. Dimostrare che la mappa $U \to U$ che associa $x \mapsto x^n$ è un automorfismo.

Soluzione. Che è un omomorfismo è chiaro. Mostriamo la surgettività: sia $u \in U$ e cerchiamo x tale che $x^n = u$. Per un tale x deve valere $x^n \equiv 1 \pmod{\mathfrak{m}}$ per definizione di U, e dunque cerchiamo le radici di $f(x) = x^n - 1$ in $A/\mathfrak{m}$. Dato che n è coprimo con $\operatorname{char} A/\mathfrak{m}$, allora guardando la derivata $f'(x)$ si ottiene che 1 è radice semplice di f, per cui possiamo spezzare $f(x) = (x - 1)g(x)$, e i due fattori sono monici e primi fra loro. Per il Lemma di Hensel riusciamo a sollevare e scrivere

$$F(x) = x^n - u = (x - \alpha)G(x)$$

Dunque α è radice di $x^n - u$, cioè $\alpha^n = u$, e $\alpha \in U$ perché $\alpha \equiv 1 \pmod{\mathfrak{m}}$.

[29] Vedi Proposizione 4.13.

[30] Se $\operatorname{char} A/\mathfrak{m} = 0$ va bene qualunque n.

Occupiamoci ora dell'iniettività. Supponiamo $u^n = 1$. Possiamo scrivere $u = 1 + a$, con $a \in \mathfrak{m}$, e dunque

$$u^n = (1+a)^n \equiv 1 + na \pmod{\mathfrak{m}^2}$$

e da $u^n = 1$ segue subito $na \equiv 0 \pmod{\mathfrak{m}^2}$. Tuttavia n è invertibile in $A/\mathfrak{m}$ perché è primo con la sua caratteristica, per cui possiamo scrivere $kn = 1 + m_1$, e da $kna \equiv 0 \pmod{\mathfrak{m}^2}$ segue $(1 + m_1)a \equiv 0 \pmod{\mathfrak{m}^2}$ e dunque $a \equiv -am_1 \equiv 0 \pmod{\mathfrak{m}^2}$. Dunque se $a \in \mathfrak{m}$ allora $a \in \mathfrak{m}^2$, e induttivamente $a \in \bigcap \mathfrak{m}^j$. Quest'intersezione deve però essere 0 perché è il Ker della mappa $A \to \hat{A}$, che è un isomorfismo perché A è completo[31]. □

[31] Vedi Proposizione 4.14 e Definizione 4.15.

Capitolo 5

Teoria della Dimensione

5.1 Dimensione degli Anelli Noetheriani Locali

La dimensione di Krull è bella e tutto quanto, ma non è che sia sempre facilissima da calcolare. In qualche caso (guardare il titolo sella sezione) però salta fuori che si possono definire altre due nozioni di dimensione, e che queste coincidono con la dimensione di Krull, il che significa avere due maniere in più per calcolarla. L'ipotesi di località ha il suo senso: magari la dimensione che ci interessa è quella del localizzato dell'anello coordinato di una varietà in un punto...[1]

Notazione 5.1. Se un anello è locale il suo ideale massimale sarà $\mathfrak{m}$.

Proposizione 5.2. Siano A locale noetheriano, $\mathfrak{q}$ un ideale $\mathfrak{m}$-primario, M un A-modulo finitamente generato e $\{M_n\}$ una $\mathfrak{q}$-filtrazione stabile di M. Allora vale che:

1. M/M_n è di lunghezza finita, cioè ammette serie di composizione, per ogni $n \geq 0$;

2. $\ell(M/M_n)$ è definitivamente un polinomio $g(n)$ di grado $\leq s$, dove s è il minimo numero di generatori di $\mathfrak{q}$;

3. Il grado e il coefficiente direttore di $g(n)$ dipendono solo da M e da $\mathfrak{q}$, e non dalla filtrazione M_n, purché sia stabile.

Dimostrazione.

1. L'idea è vedere che $A/\mathfrak{q}$ è artiniano, usare questo fatto per recuperare una serie di composizione per ogni M_i/M_{i+1} e incollarle tutte per

[1] Se queste chiacchiere introduttive generano confusione possono essere tranquillamente ignorate.

ottenerne una per M/M_n. Veniamo ai dettagli: consideriamo l'anello e il modulo graduato indotti da $\mathfrak{q}$ e dalla filtrazione

$$\mathrm{gr}_{\mathfrak{q}}(A) = \bigoplus_{i=0}^{\infty} {\mathfrak{q}^i}\big/{\mathfrak{q}^{i+1}} \qquad \mathrm{gr}(M) = \bigoplus_{i=0}^{\infty} {M_i}\big/{M_{i+1}}$$

Dato che $\{M_n\}$ è una $\mathfrak{q}$-filtrazione è facile vedere che $\mathrm{gr}(M)$ possiede una naturale struttura di $\mathrm{gr}_{\mathfrak{q}}(A)$-modulo graduato. L'anello $(\mathrm{gr}_{\mathfrak{q}}(A))_0 = A/\mathfrak{q}$ è noetheriano perché quoziente di un noetheriano, e ha anche dimensione 0: infatti il suo unico ideale massimale è $\overline{\mathfrak{m}}$, e per ogni $\overline{\mathfrak{p}}$ primo tale che $0 \subseteq \overline{\mathfrak{p}} \subseteq \overline{\mathfrak{m}}$ vale $\mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$, da cui passando ai radicali otteniamo $\mathfrak{m} = \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{p}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$. Allora per il Teorema di Caratterizzazione degli Anelli Artiniani $A/\mathfrak{q}$ è artiniano, e ne segue che ogni M_n/M_{n+1}, in quanto $A/\mathfrak{q}$-modulo[2] finitamente generato su un anello artiniano, è sia noetheriano che artiniano e dunque per il Teorema 3.10 ammette serie di composizione, cioè $\ell(M_n/M_{n+1}) < +\infty$. Ora basta scrivere le successioni esatte[3]

$$0 \to {M_i}\big/{M_{i+1}} \to {M}\big/{M_{i+1}} \to {M}\big/{M_i} \to 0$$

prendere quella con $i = 1$, prendere una serie di composizione per M/M_1, incollarla[4] a quella per M_1/M_2, ottenendone una per M/M_2, prendere la successione esatta con $i = 2$ e iterare fino ad ottenere una serie di composizione per M/M_n.

2. Siamo nelle ipotesi del Teorema di Hilbert-Serre. Infatti $\mathrm{gr}(M)$ è un $\mathrm{gr}_{\mathfrak{q}}(A)$-modulo finitamente generato[5], e abbiamo già visto[6] che $\mathrm{gr}_{\mathfrak{q}}(A)$ è noetheriano in quanto si può scrivere come $A/\mathfrak{q}$ algebra:

$$\mathrm{gr}_{\mathfrak{q}} A = A/\mathfrak{q}[\overline{x_1}, \ldots, \overline{x_s}]$$

dove $x_1, \ldots, x_s$ generano $\mathfrak{q} \subseteq A$. Quindi, per il Corollario 3.30, definitivamente $\ell(M_n/M_{n+1}) = f(n)$, con f polinomio di grado $\leq s-1$. A noi però interessa $\ell(M/M_n)$. Chiamiamo $\ell_n = \ell(M/M_n)$ e notiamo che per $n \geq \tilde{n}$ abbiamo la relazione $\ell_{n+1} - \ell_n = f(n)$. Definendo

$$p(n) = \begin{cases} \ell_n & \text{per } n \geq \tilde{n} \\ \ell_{\tilde{n}} - \sum_{t=n}^{\tilde{n}-1} f(t) & \text{per } n < \tilde{n} \end{cases}$$

[2] A priori sappiamo solo che è un A-modulo, ma dato che $\{M_n\}$ è una $\mathfrak{q}$-filtrazione abbiamo $\mathfrak{q} \subseteq \mathrm{Ann}(M_n/M_{n+1})$.

[3] Di A-moduli, ma gli A-sottomoduli di M_i/M_{i+1} coincidono con gli $A/\mathfrak{q}$-sottomoduli.

[4] Cfr. dimostrazione della Proposizione 3.14.

[5] La situazione è analoga a quella della Proposizione 4.28: abbiamo già detto che gli M_i/M_{i+1} sono $A/\mathfrak{q}$ moduli finitamente generati. Allora basta iniziare a raccogliere i loro generatori finché, per un certo i, la filtrazione si stabilizza. A quel punto basta usare gli elementi dei $\mathfrak{q}_j/\mathfrak{q}_{j+1}$ con i finiti generatori raccolti.

[6] Proposizione 3.22.

abbiamo allora $p(n+1) - p(n) = f(n)$ *per ogni* n, e non solo definitivamente. Per concludere ci serve il fatto che

Lemma 5.3. Siano $p, f\colon \mathbb{N} \to \mathbb{Z}$ funzioni tali che $p(n+1) - p(n) = f(n)$. Allora $p(n) \in \mathbb{Q}[n]$ se e solo se $f(n) \in \mathbb{Q}[n]$. Inoltre, se ciò accade, $\deg p = \deg f + 1$.

Fatto questo abbiamo finito, perché $f \in \mathbb{Q}[n]$, e allora $p(n)$ è un polinomio $g(n)$ definitivamente pari a ℓ_n di grado al più

$$\deg f + 1 \leq s - 1 + 1 = s$$

Dimostrazione del Lemma. Una freccia è ovvia: se $p(n) \in \mathbb{Q}[n]$ anche $f(n) = p(n+1) - p(n) \in \mathbb{Q}[n]$. Viceversa, se $f(n) \in \mathbb{Q}[n]$, per ipotesi possiamo scrivere

$$p(n) = p(0) + \sum_{t=0}^{n-1} f(t)$$

Pensiamo ora $f(x) \in \mathbb{Q}[x]$ come polinomio formale. Ogni polinomio a coefficienti in $\mathbb{Q}$ può essere pensato come generato da $\binom{x}{0}, \binom{x}{1}, \binom{x}{2}, \ldots$, perché $\binom{x}{n}$ è[7] un polinomio in x di grado n e quindi basta dimostrare la tesi per i polinomi $\binom{x}{k}$. Studiamo quindi $\sum_{t=0}^{n-1} \binom{t}{k}$, che è noto essere uguale a $\binom{n}{k+1}$, perché è sommare su una diagonale del triangolo di Tartaglia[8]. Dato che $\binom{n}{k+1}$ ha grado $k+1$ in n abbiamo concluso. □

3. Se $\{\widetilde{M}_n\}$ è un'altra filtrazione stabile di M possiamo ripetere il ragionamento precedente e ottenere un altro polinomio $\widetilde{g}(n)$ che è definitivamente $\ell(M/\widetilde{M}_n)$. Per la Proposizione 4.29, due filtrazioni $\mathfrak{q}$-stabili hanno differenze limitate, cioè esiste n_0 tale che per ogni n valga $M_{n+n_0} \subseteq \widetilde{M}_n$ e $\widetilde{M}_{n+n_0} \subseteq M_n$. Ne segue che, usando il primo punto del Teorema 3.9, per n sufficientemente grande valgono sia $g(n+n_0) \geq \widetilde{g}(n)$ che $\widetilde{g}(n+n_0) \geq g(n)$. Dunque g, $\widetilde{g}$ hanno lo stesso grado e coefficiente direttore, come si vede subito chiamando A il rapporto fra i coefficienti direttori e scrivendo

$$A = \lim_{n\to\infty} \frac{g(n+n_0)}{\widetilde{g}(n)} \geq 1 \qquad \frac{1}{A} = \lim_{n\to\infty} \frac{\widetilde{g}(n+n_0)}{g(n)} \geq 1 \qquad \square$$

Gli altri coefficienti possono essere diversi, ma non ci interesseranno.

Definizione 5.4. Denotiamo con $\chi_{\mathfrak{q}}^{M}(n)$ il polinomio $g(n)$ associato alla filtrazione standard $\{\mathfrak{q}^n M\}$.

[7] Ad esempio $\binom{x}{3} = \frac{x(x-1)(x-2)}{3!}$.

[8] Basta fare un esempio per convincersene e, volendo, scrivere un dimostrazione formale.

Per quanto visto, definitivamente $\chi_{\mathfrak{q}}^M(n) = \ell(M/\mathfrak{q}^n M)$. Se $A = M$, allora $\chi_{\mathfrak{q}}^A(n)$ si chiama *polinomio caratteristico dell'ideale* $\mathfrak{m}$*-primario* $\mathfrak{q}$, e abbiamo visto che il suo grado è minore o uguale del minimo numero di generatori di $\mathfrak{q}$. Ci piacerebbe che questo polinomio fosse associato all'anello e basta, senza dover dipendere da ideali. E in effetti qualcosa non dipende da $\mathfrak{q}$:

Proposizione 5.5. Sia A un anello locale noetheriano con ideale massimale $\mathfrak{m}$ e sia $\mathfrak{q}$ un ideale $\mathfrak{m}$-primario. Allora $\deg \chi_{\mathfrak{q}}^A(n) = \deg \chi_{\mathfrak{m}}^A(n)$.

Dimostrazione. Per noetherianità $\mathfrak{q}$ contiene una potenza del suo radicale. Allora da $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ otteniamo $\mathfrak{m}^{rn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$ e definitivamente, dato che stiamo parlando delle lunghezze dei quozienti $A/\mathfrak{m}^{rn}$, $A/\mathfrak{q}^n$, $A/\mathfrak{m}^n$, si ha quindi (i gradi sono da intendersi come polinomi in n)

$$\deg \chi_{\mathfrak{m}}^A(rn) \geq \deg \chi_{\mathfrak{q}}^A(n) \geq \deg \chi_{\mathfrak{m}}^A(n)$$

e questo può essere vero solo se i due polinomi hanno lo stesso grado. □

Dunque tutti i $\chi_{\mathfrak{q}}^A$, anche se diversi, hanno lo stesso grado, cioè $\deg \chi_{\mathfrak{m}}^A(n)$. Siamo pronti per dare la prossima

Definizione 5.6. Sia A un anello locale noetheriano. Poniamo $d(A) = \deg \chi_{\mathfrak{q}}^A(n)$, con $\mathfrak{q}$ ideale $\mathfrak{m}$-primario qualsiasi.

Osservazione 5.7. L'invariante $d(A)$ coincide con l'ordine del polo della serie di Hilbert di $\mathrm{gr}_{\mathfrak{m}}(A)$. Questo si può vedere ripercorrendo la dimostrazione della Proposizione 5.2 e leggendo attentamente l'enunciato del Corollario 3.30.

Dopo d e $\dim_{\mathrm{Krull}}$ presentiamo il terzo protagonista di questa sezione:

Definizione 5.8. Sia A un anello locale noetheriano. Definiamo $\delta(A)$ come il minimo numero di generatori di un ideale $\mathfrak{m}$-primario.

Attenzione: sappiamo già che $\delta(A) \geq d(A)$. Infatti se $\delta(A) = s$ sia $\mathfrak{q} = (x_1, \ldots, x_s)$ l'ideale $\mathfrak{m}$-primario che realizza la definizione. Consideriamo l'anello $\mathrm{gr}_{\mathfrak{m}}(A)$; questo è generato come $A/\mathfrak{q}$-algebra da $\overline{x_1}, \ldots, \overline{x_s}$ e per la Proposizione 5.2 il grado di $\chi_{\mathfrak{q}}^A(n)$ è $\leq s$, da cui la disuguaglianza. La parte difficile è $\delta(A) \leq \dim_{\mathrm{Krull}}$, di cui ci occuperemo alla fine, mentre ora dimostriamo la disuguaglianza $\dim_{\mathrm{Krull}}(A) \leq d(A)$. Ci servirà il fatto che

Proposizione 5.9. Siano A, $\mathfrak{m}$, $\mathfrak{q}$ come sopra, M un A-modulo finitamente generato, $x \in A$ un elemento che non annulla alcun elemento del modulo[9] e $M' = M/xM$. Allora $\deg \chi_{\mathfrak{q}}^{M'} \leq \deg \chi_{\mathfrak{q}}^M - 1$.

[9] Che, nel caso $M = A$, vuol dire che x non è un divisore di 0.

Dimostrazione. Sia $N = xM$. Come A-modulo $N \cong M$, perché l'omomorfismo $M \to M$ dato dalla moltiplicazione per x è iniettivo per ipotesi. Consideriamo la filtrazione $N_n = N \cap \mathfrak{q}^n M$ e la successione esatta

$$0 \to N \xrightarrow{i} M \to M' \to 0$$

Questa passa al quoziente diventando la successione esatta

$$0 \to {}^{N}\!/_{N_n} \to {}^{M}\!/_{\mathfrak{q}^n M} \to {}^{M'}\!/_{\mathfrak{q}^n M'} \to 0$$

utilizzando il fatto che $\pi(\mathfrak{q}^n M) = \mathfrak{q}^n M'$. Sia $g(n) = \ell(N/N_n)$. Dato che ℓ è additiva abbiamo, definitivamente,

$$\chi_{\mathfrak{q}}^{M'}(n) = \chi_{\mathfrak{q}}^{M}(n) - g(n)$$

Per Artin-Rees, la N_n è una filtrazione $\mathfrak{q}$-stabile di N, che però è isomorfo a M, per cui per il terzo punto della Proposizione 5.2, $g(n)$ e $\chi_{\mathfrak{q}}^{M}(n)$ hanno lo stesso grado e coefficiente direttore. Dunque nell'equazione sopra i loro monomi di grado massimo si cancellano e $\deg \chi_{\mathfrak{q}}^{M'}(n) \leq \deg \chi_{\mathfrak{q}}^{M}(n) - 1$. □

Corollario 5.10. Sia A un anello locale noetheriano e x non divisore di 0. Allora $d(A/(x)) \leq d(A) - 1$.

Questo ci dice che negli anelli noetheriani locali quozientare per le cose giuste è effettivamente un buon passo induttivo. Ne approfittiamo subito:

Teorema 5.11. $d(A) \geq \dim_{\text{Krull}}(A)$.

Dimostrazione. Come anticipato procediamo per induzione su $d = d(A)$. Se $d = 0$ allora definitivamente $\ell(A/\mathfrak{m}^n)$ è costante per cui $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Per il lemma di Nakayama, $\mathfrak{m}^n = 0$, e se quindi se $\mathfrak{p}$ è un primo di A abbiamo $\mathfrak{m}^n = (0) \subseteq \mathfrak{p} \subseteq \mathfrak{m}$. Passando ai radicali scopriamo che $\mathfrak{m}$ è l'unico primo e quindi $\dim(A) = 0$. Sia ora $d > 0$ e consideriamo una catena di primi

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$$

Sia $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$ e consideriamo il quoziente $A' = A/\mathfrak{p}_0$, che è un dominio perché $\mathfrak{p}_0$ è primo. L'immagine x' di x in A' non è quindi un divisore di 0, e per il Corollario 5.10 vale $d(A'/(x')) \leq d(A') - 1$. Se $\mathfrak{m}'$ è l'ideale massimale di A', allora $A'/(\mathfrak{m}')^n$ è immagine omomorfa di $A/\mathfrak{m}^n$; dunque $\ell(A/\mathfrak{m}^n) \geq \ell(A'/(\mathfrak{m}')^n)$, perché la lunghezza è una funzione additiva. Passando ai gradi dei rispettivi polinomi caratteristici abbiamo $d(A) \geq d(A')$. Riepilogando,

$$d(A'/(x')) \leq d(A') - 1 \leq d(A) - 1 = d - 1$$

Quindi per ipotesi induttiva, la lunghezza di una catena di primi in $A'/(x')$ non supera $d - 1$, ma le immagini $\overline{\mathfrak{p}_1}, \ldots, \overline{\mathfrak{p}_r}$ in $A'/(x')$ formano una catena di lunghezza $r - 1$, quindi $r - 1 \leq d - 1$, cioè $r \leq d$, che è la tesi. □

Quindi, dato che $d(A)$ è finito per definizione, abbiamo scoperto che finché si parla di anelli noetheriani locali non c'è da preoccuparsi di brutte bestie come il Controesempio di Nagata:

Corollario 5.12. Gli anelli locali noetheriani hanno dimensione di Krull finita.

Corollario 5.13. Ogni ideale primo in un anello noetheriano ha altezza finita. In particolare l'insieme degli ideali primi di un anello noetheriano soddisfa la d.c.c.

Dimostrazione. Per la prima parte basta andare in $A_{\mathfrak{p}}$. Per la seconda, se la catena è $\mathfrak{p}_0 \supsetneq \dots$ basta andare in $A_{\mathfrak{p}_0}$. □

Chiudiamo il cerchio (di disuguaglianze) con il prossimo

Teorema 5.14. $\dim_{\text{Krull}}(A) \geq \delta(A)$.

Dimostrazione. Poniamo $d = \dim_{\text{Krull}}(A)$ e mostriamo che esiste un ideale $\mathfrak{m}$-primario in A generato da d elementi per induzione su d. Se $d = 0$ l'anello A è artiniano e per un qualche n vale[10] $\mathfrak{m}^n = (0)$. Dunque (0) è $\mathfrak{m}$-primario, e dato che (0) ha 0 generatori $\delta(A) = 0$. Per $d \geq 1$ invece costruiamo $x_1, \dots, x_d$ in modo che $\forall i \leq d$ valga la proposizione

$$\mathcal{P}(i) \equiv \text{“ogni ideale primo contenente } (x_1, \dots, x_i) \text{ ha altezza} \geq i\text{”}$$

Supponiamo di aver già costruito $x_1, \dots, x_{i-1}$ per cui valga $\mathcal{P}$ e vediamo come costruire x_i. Siano $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ i primi minimali[11] dell'ideale $(x_1, \dots, x_{i-1})$ tali che $\text{ht}(\mathfrak{p}_j) = i - 1$, se esistono[12]. Dato che $i - 1 < d = \dim_{\text{Krull}}(A) = \text{ht}(\mathfrak{m})$, per ogni j vale $\mathfrak{m} \supsetneq \mathfrak{p}_j$, quindi per il Prime Avoidance Lemma[13], $\mathfrak{m} \supsetneq \bigcup_{j=1}^{s} \mathfrak{p}_j$. Scegliamo dunque $x_i \in \mathfrak{m} \setminus \bigcup \mathfrak{p}_j$ e verifichiamo che valga $\mathcal{P}(i)$. Un primo $\mathfrak{q}$ contenente $(x_1, \dots, x_i)$ conterrà anche un primo minimale $\mathfrak{p}$ di $(x_1, \dots, x_{i-1})$. Se $\mathfrak{p}$ è uno dei $\mathfrak{p}_j$, cioè ha altezza $i - 1$, allora $x_i \in \mathfrak{q} \setminus \mathfrak{p}_j$ testimonia che $\mathfrak{q} \supsetneq \mathfrak{p}$, e quindi $\text{ht}(\mathfrak{q}) \geq i$. Altrimenti, $\text{ht}(\mathfrak{p}) \geq i$, e allora $\text{ht}(\mathfrak{q}) \geq \text{ht}(\mathfrak{p}) \geq i$. Iterando troviamo l'ideale $J = (x_1, \dots, x_d)$, e se mostriamo che è $\mathfrak{m}$-primario abbiamo finito. Se I è un primo minimale che lo contiene, allora $\text{ht}(I) \geq d$, per cui $I = \mathfrak{m}$, altrimenti avremmo $d = \text{ht}(\mathfrak{m}) > \text{ht}(I) \geq d$. Dunque $\sqrt{J} = \mathfrak{m}$, perché il suo radicale è l'intersezione dei primi che lo contengono e abbiamo detto che c'è solo $\mathfrak{m}$. D'altronde se $\sqrt{J}$ è massimale J è primario[14]. □

[10] Vedi Proposizione 3.3, il nilradicale è l'intersezione dei primi e qui di primi non ce ne sono molti....

[11] Nel senso della decomposizione primaria o nel senso dei primi minimali che includono l'ideale: nelle nostre ipotesi le due nozioni coincidono. Vedi [2], Proposizione 4.6 e Teorema 7.13.

[12] Potrebbero avere tutti altezza $\geq i$. Comunque, come sarà chiaro fra poco, anche se succede non è un problema, anzi.

[13] Proposizione 1.11 in [2].

[14] Vedi Proposizione 4.2 in [2].

Riassiumiamo tutto il lavoro fatto finora nel seguente

Teorema 5.15 (della Dimensione)**.** Sia A un anello locale noetheriano e $\mathfrak{m}$ il suo ideale massimale e sia $\mathfrak{q}$ un ideale $\mathfrak{m}$-primario. Allora coincidono

- $\dim_{\text{Krull}}(A)$
- $\deg(\chi^A_{\mathfrak{m}}(n))$, dove $\chi^A_{\mathfrak{m}}(n)$ è definitivamente uguale a $\ell(A/\mathfrak{m}^n)$
- $\deg(\chi^A_{\mathfrak{q}}(n))$, dove $\chi^A_{\mathfrak{q}}(n)$ definitivamente uguale a $\ell(A/\mathfrak{q}^n)$
- $\delta(A)$

Corollario 5.16. Sia A un anello locale noetheriano. Allora $\dim(A) \leq \dim_K(\mathfrak{m}/\mathfrak{m}^2)$.

Dimostrazione. Per il Lemma di Nakayama[15], se $\overline{x_1}, \ldots, \overline{x_s}$ sono una base di $\mathfrak{m}/\mathfrak{m}^2$, gli x_i generano $\mathfrak{m}$. Quindi $\dim A \leq s = \dim_K(\mathfrak{m}/\mathfrak{m}^2)$. □

Corollario 5.17 (Teorema di Krull sull'Altezza degli Ideali)**.** Sia A noetheriano[16] e siano $x_1, \ldots, x_r \in A$. Allora ogni ideale primo minimale di $(x_1, \ldots, x_r)$ ha altezza $\leq r$.

Dimostrazione. Sia $\mathfrak{p}$ un primo minimale di $I = (x_1, \ldots, x_r)$. Localizzando per $\mathfrak{p}$, l'ideale $(x_1, \ldots, x_r)^e$ è $\mathfrak{p}^e$-primario, dunque $r \geq \delta(A_{\mathfrak{p}}) = \dim A_{\mathfrak{p}} = \text{ht}(\mathfrak{p})$. □

Nell'Esempio 2.12, l'ideale $\mathfrak{m}_2$ era generato da due elementi e quindi aveva altezza esattamente 2 per quanto dimostrato ora. Enunciamo separatamente un caso particolare del Teorema precedente per ragioni di fama.

Corollario 5.18 (Teorema dell'Ideale Principale di Krull)**.** Sia A un anello noetheriano e sia $x \in A$ non divisore di 0 e non invertibile. Allora ogni ideale primo minimale $\mathfrak{p}$ di (x) ha altezza esattamente 1.

Dimostrazione. Come prima $\text{ht}(\mathfrak{p}) \leq 1$ perché l'ideale $(x)^e$ è $\mathfrak{p}^e$-primario in $A_{\mathfrak{p}}$. Se fosse 0, $\mathfrak{p}$ sarebbe un primo minimale di (0), ma per la teoria della decomposizione primaria[17] l'insieme dei divisori di 0 coincide con l'unione dei primi minimali. Allora $x \in \mathfrak{p}$ dovrebbe essere un divisore di 0, contro le ipotesi. □

Notiamo che avevamo già dimostrato nella Proposizione 2.13 che, se A è noetheriano, ogni primo $\mathfrak{p}$ propriamente contenuto in un ideale proprio e principale ha altezza 0. La Proposizione 5.9 può essere rafforzata:

[15] Vedi Proposizione 2.8 in [2].
[16] Non necessariamente locale.
[17] Vedi sempre [2], Proposizione 4.6 e Teorema 7.13.

Corollario 5.19. Sia A un anello locale noetheriano e $x \in \mathfrak{m}$. Allora $\dim A/(x) \geq \dim(A) - 1$. Se inoltre x non è divisore di 0 vale l'uguaglianza.

Dimostrazione. Sia $m = \dim A/(x)$ e siano $x_1, \ldots, x_m \in A$ tali che le loro proiezioni generino in $A/(x)$ un ideale $\mathfrak{m}/(x)$-primario. Allora $(x, x_1, \ldots, x_m)$ è un ideale $\mathfrak{m}$-primario, e quindi $\dim A \leq \dim A/(x) + 1$. □

Questo è molto bello perché ora, quando quozientiamo un anello locale noetheriano per un non divisore di zero, sappiamo esattamente cosa succede alla dimensione.

5.2 Anelli Locali Regolari

Nel calcolo di $\delta(A)$ non è detto che si possa prendere $\mathfrak{q} = \mathfrak{m}$: ad esempio potrebbe esserci (e in effetti c'è) un anello di dimensione 7 dove $\mathfrak{m}$ non può essere generato da meno di 8 elementi. Quand'è che proprio $\mathfrak{m}$ è generato da $\delta(A)$ elementi? Questi si chiamano *anelli locali regolari*, e il "premio geometrico" è che sono quelli associati ai punti non singolari di una varietà[18].

Definizione 5.20. Un anello noetheriano locale di dimensione d si dice *locale regolare* se il suo ideale massimale è generato da d generatori. In genere dire "locale regolare" sottintende noetheriano.

Esempio 5.21. Sia $A = \mathbb{C}[x, y]/(y^2 - x^3)$ e consideriamo i localizzati $B = A_{(x-1,y-1)}$ e $C = A_{(x,y)}$.

Notiamo intanto che $y^2 - x^3$ è irriducibile; sappiamo poi che $\dim \mathbb{C}[x, y] = 2$ e quindi $\dim A = 1$ per la Proposizione 2.6. Dato che A è un dominio, per il Corollario 2.9 i suoi massimali hanno tutti la stessa altezza, e dunque vale $\dim B = \dim C = 1$. In $A_{(x-1,y-1)}$ l'ideale massimale $(x - 1, y - 1)^e$ sembrerebbe generato da 2 elementi, e uno direbbe che quindi l'anello non è regolare. Tuttavia qua dentro vale

$$(y + 1)(y - 1) = (y^2 - 1) = x^3 - 1$$

E dato che $y + 1$ è invertibile in B perché $y + 1 \notin (x - 1, y - 1)$ abbiamo

$$y - 1 = (y + 1)^{-1}(x - 1)(x^2 + x + 1) \in (x - 1)^e$$

per cui B è regolare. C invece no:

Esercizio 5.22. Verificare che $(x, y)^e$ non è principale.

L'obiettivo è ora mostrare che la definizione di anello locale regolare è equivalente alle seguenti condizioni:

[18] Detto così sembra piovuto dal cielo, ma se uno va leggersi le definizioni di punto singolare e spazio tangente in [14] e guarda il Corollario 5.16 o direttamente il Teorema 5.25 probabilmente gli si accende una lampadina.

1. $\operatorname{gr}_{\mathfrak{m}} A \cong K[T_1, \dots, T_{\dim A}]$ (implicherà che A è un dominio)
2. $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = \dim A$

Il lavoro sporco lo fa la seguente

Proposizione 5.23. Sia A un anello locale noetheriano di dimensione d e sia $\mathfrak{q} = (x_1, \dots, x_d)$ un ideale $\mathfrak{m}$-primario[19]. Sia $f(T_1, \dots, T_d) \in A[T_1, \dots, T_d]$ un polinomio omogeneo di grado s e supponiamo che $f(x_1, \dots, x_d) \in \mathfrak{q}^{s+1}$. Allora i coefficienti di f appartengono a $\mathfrak{m}$.

Dimostrazione. Se[20] $s = 0$ allora $f \in A$, cioè f è costante, e allora si ha ovviamente $f \in \mathfrak{q}^1 \subseteq \mathfrak{m}$. Se $s > 0$ consideriamo la mappa surgettiva di anelli graduati[21]

$$\vartheta \colon {}^{A}\!/_{\mathfrak{q}}[T_1, \dots, T_d] \to \operatorname{gr}_{\mathfrak{q}}(A) \qquad \vartheta(T_i) = \overline{x_i}$$

dove $\overline{x_i}$ è[22] x_i modulo $\mathfrak{q}^2$. Consideriamo $\bar{f} \in A/\mathfrak{q}[T_1, \dots, T_d]$: per ipotesi[23] $\bar{f} \in \operatorname{Ker} \vartheta$. Supponiamo per assurdo che qualche coefficiente di f sia invertibile (ossia $\notin \mathfrak{m}$). Allora $\bar{f}$ non è[24] un divisore di 0. Ne segue che, se $\operatorname{op}(-)$ indica l'ordine del polo della serie di Hilbert in 1,

$$\operatorname{op}(\operatorname{gr}_{\mathfrak{q}} A) \leq \operatorname{op}\left(\big((A/\mathfrak{q})[T_1, \dots, T_d]\big)/(\bar{f})\right) = \operatorname{op}(A/\mathfrak{q}[T_1, \dots, T_d]) - 1 = d - 1$$

Dove

- Il secondo termine da sinistra è ancora un anello graduato, e quindi ha senso parlare op. Questo è facile da verificare tenendo a mente che $\bar{f}$ è omogeneo.
- La disuguaglianza a sinistra si dimostra ricordandosi come gli ordini dei poli dipendono dalle lunghezze dei sottomoduli omogenei. Dato che a sinistra abbiamo $\operatorname{gr}_{\mathfrak{q}} A \cong \big((A/\mathfrak{q})[T_1, \dots, T_d]\big)/\operatorname{Ker} \vartheta$ e a destra, dato che $f \in \operatorname{Ker} \vartheta$, stiamo quozientando per un sottomodulo più piccolo, per additività le lunghezze degli $(\dots)_n$ non possono diminuire.

[19] Dunque $x_1, \dots, x_d$ realizzano $\delta(A)$, il minimo numero di generatori di un ideale $\mathfrak{m}$-primario. A volte vengono chiamati un *sistema di parametri*.

[20] Qui [2] non si pone il problema, ma se $s = 0$ la Proposizione 3.31 non funziona, quindi meglio sistemare questo caso all'inizio e non pensarci più, come suggerito in [10]. Qualcuno potrebbe storcere il naso anche davanti al caso $d = 0$. Tuttavia $d = 0$ implica $s = 0$ perché allora f è un polinomio in 0 variabili, cioè $f \in A$.

[21] Si intende che manda omogenei in omogenei. Nel nostro caso rispetta anche il grado, ma *non* è richiesto. Nella parte di algebra omologica lavoreremo anche con mappe che mandano omogenei in omogenei ma cambiano il grado.

[22] Occhio: su [2] qui c'è un typo e invece di $\mathfrak{q}^2$ c'è scritto $\mathfrak{q}$. Chiaramente $x_i \equiv 0 \pmod{\mathfrak{q}}$.

[23] Basta ricordarsi che il "pezzo" di grado s in $\operatorname{gr}_{\mathfrak{q}}(A)$ è $\mathfrak{q}^s/\mathfrak{q}^{s+1}$.

[24] Per l'Esercizio 3 del Capitolo I di [2] (o meglio, per la sua versione in più variabili) sappiamo che $g \in B[x]$ è un divisore di 0 se e solo se è annullato da un $b \in B$ non nullo.

- L'uguaglianza al centro è vera per la Proposizione 3.31. Il k della Proposizione in questo caso è s, e le ipotesi sono soddisfatte perché $s > 0$ e $\operatorname{OP}\big(((A/\mathfrak{q})[T_1, \ldots, T_d])/(\bar{f})\big) \geq \operatorname{OP}(\operatorname{gr}_{\mathfrak{q}} A) = d \geq 1$ per quanto osservato in nota.

- L'uguaglianza a destra segue dal fatto che $(A/\mathfrak{q}[T_1, \ldots, T_d])_n$ è libero sui monomi di grado n, che sono $\binom{d+n-1}{d-1}$, e quindi[25] ha lunghezza $\ell(A/\mathfrak{q})\binom{d+n-1}{d-1}$. Dunque la serie di Hilbert che ci interessa è $\sum \ell(A/\mathfrak{q})\binom{d+n-1}{d-1} t^n = \ell(A/\mathfrak{q})(1-t)^{-d}$, ed è evidente che il suo polo in 1 ha ordine d.

Questo è assurdo perché per l'Osservazione 5.7 e il Teorema della Dimensione $\operatorname{OP}(\operatorname{gr}_{\mathfrak{q}} A) = d(A) = \delta(A) = d$. □

Osservazione 5.24. Nella Proposizione precedente, invece che con gli ordini dei poli, uno potrebbe anche lavorare con la dimensione di Krull, e la disuguaglianza $\dim(\operatorname{gr}_{\mathfrak{q}} A) \leq d-1$ si riesce comunque ad tirare fuori con una quantità ragionevole di fatica (un pezzo è il Corollario 5.19). Il problema è che l'uguaglianza che fornisce l'assurdo è molto più laboriosa da ottenere (e comunque in un modo o nell'altro dagli ordini dei poli non si scappa; ma dalla Proposizione 3.31 sì.). Vedi Esercizio A.10.

Teorema 5.25. Siano A un anello locale noetheriano di dimensione d, $\mathfrak{m}$ il suo ideale massimale e $K = A/\mathfrak{m}$. Allora sono equivalenti:

1. $\operatorname{gr}_{\mathfrak{m}} A \cong K[T_1, \ldots, T_d]$
2. $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = d$
3. $\mathfrak{m}$ è generato da d elementi (ovvero A è locale regolare).

Dimostrazione.

$(1 \Rightarrow 2)$ $\mathfrak{m} = (T_1, \ldots, T_d)$.

$(2 \Rightarrow 3)$ Nakayama[26] e definizione di $\delta(A)$ (cfr. Corollario 5.16).

$(3 \Rightarrow 1)$ Usiamo la $\vartheta\colon A/\mathfrak{m}[T_1, \ldots, T_d] \to \operatorname{gr}_{\mathfrak{m}} A$ della Proposizione precedente, che è surgettiva per definizione. Per la Proposizione precedente se $\bar{f} \in \operatorname{Ker}\vartheta$ allora $\bar{f}$ ha tutti i coefficienti non invertibili, cioè $\bar{f} = 0$ perché $A/\mathfrak{m}$ è un campo. Ma allora ϑ è un isomorfismo. □

Proposizione 5.26. Se $\bigcap_{j=1}^{\infty} I^j = (0)$ allora $\operatorname{gr}_I(A)$ dominio implica A dominio.

[25] La verifica di questa cosa è lasciata al lettore.
[26] Vedi Proposizione 2.8 in [2].

Dimostrazione. Supponiamo per assurdo che esistano $x, y \in A$ non nulli e tali che $xy = 0$. Dato che $\bigcap I^j = (0)$ esistono n tale che $x \in I^n \setminus I^{n+1}$ ed m tale che $y \in I^m \setminus I^{m+1}$. Dunque in $\mathrm{gr}_I(A)$ abbiamo che $\bar{x} \in I^n/I^{n+1}$ e $\bar{y} \in I^m/I^{m+1}$ sono non nulli. Ora $\bar{x}\bar{y} \in I^{n+m}/I^{n+m+1}$ dovrebbe essere non nullo perché $\mathrm{gr}_I(A)$ è un dominio, ma $\bar{x}\bar{y} = \overline{xy} = 0$ perché $xy = 0$ in A. □

Corollario 5.27. Gli anelli locali regolari sono sempre domini.

Dimostrazione. Per il Teorema 5.25 $\mathrm{gr}_{\mathfrak{m}} A \cong K[T_1, \ldots, T_d]$, che è un dominio. Per il Teorema di Intersezione di Krull, o meglio per il Corollario 4.18, $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$, per cui scatta la Proposizione precedente. □

Esercizio 5.28. Siano $A = \mathbb{Z}[X, Y, Z]$, $\mathfrak{p} = (7, X, Y, Z)$, e poniamo $B = A_{\mathfrak{p}}/(Z^2 - X^3 - X - Y^2)$. L'anello B è locale regolare?

Soluzione. Mostriamo che $\dim B = 3$. Consideriamo in $\mathbb{Z}[X, Y, Z]$ la catena di ideali primi

$$(Z^2 - X^3 - X - Y^2) \subsetneq (X, Y + Z) \subsetneq (X, Y, Z) \subsetneq (7, X, Y, Z)$$

La primalità degli ultimi tre può essere vista quozientando, mentre per il primo si fa via irriducibilità in un UFD. Questa resta una catena di lunghezza 3 anche in $A_{\mathfrak{p}}$ e in B:

$$0 \subsetneq (\bar{X}, \bar{Y} + \bar{Z}) \subsetneq (\bar{X}, \bar{Y}, \bar{Z}) \subsetneq (7, \bar{X}, \bar{Y}, \bar{Z})$$

Dunque $\dim B \geq 3$. Tralasciando i "$\bar{\ }$" per non appesantire la notazione, in B vale $Z^2 - X^3 - X - Y^2 = 0$, e dunque $(Z - Y)(Z + Y) = X(X^2 + 1)$. Dato che $X^2 + 1$ non è in $\mathfrak{p}$, in B lo possiamo invertire e scrivere $\mathfrak{p} = (7, Y, Z)$ e abbiamo mostrato simultaneamente che $\dim B \leq 3$ e che B è regolare. □

Gli anelli locali regolari di dimensione 0 sono i campi: infatti sono noetheriani, di dimensione 0 (quindi artiniani) e anche domini per il Corollario 5.27, per cui il loro unico primo è (0). Se invece A è locale regolare di dimensione 1, allora il suo ideale massimale è principale $\mathfrak{m} = (x)$. In questo caso A prende il nome di *anello di valutazione discreta*. Non approfondiremo la questione, ma gli interessati possono guardare come al solito [2]. A titolo informativo comunque diciamo che

Definizione 5.29. Sia A un dominio noetheriano di dimensione 1. Se, per ogni $\mathfrak{p} \neq (0)$, l'anello $A_{\mathfrak{p}}$ è locale regolare di dimensione 1, allora A si dice un *dominio di Dedekind*.

Una proprietà importante dei domini di Dedekind è che ogni loro ideale si fattorizza unicamente come prodotto di primi.

5.3 Dimensione degli Anelli di Polinomi

Esercizio 5.30. Sia R un anello di dimensione di Krull d.

1. Dimostrare che, dato $\mathfrak{p}$ primo di R, non può accadere che esistano tre primi $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{q}_3$ di $R[X]$ tali che $\mathfrak{q}_i \cap R = \mathfrak{p}$.
2. Dimostrare che $\dim_{\text{Krull}} R[X] \leq 2d + 1$.

Soluzione. 1. Possiamo supporre $\mathfrak{q}_1 = \mathfrak{p}[X] = \mathfrak{p}^e$, altrimenti basta considerare i primi tre ideali della catena

$$\underbrace{\mathfrak{p}[X] \subsetneq \mathfrak{q}_1 \subsetneq \mathfrak{q}_2}_{\text{applicare qui}} \subsetneq \mathfrak{q}_3$$

Quozientiamo portandoci nel dominio $R/\mathfrak{p}[X] \cong R[X]/\mathfrak{p}[X]$ dove abbiamo la catena $0 \subsetneq \bar{\mathfrak{q}}_2 \subsetneq \bar{\mathfrak{q}}_3$, e poi passando al campo delle frazioni ($S = (R/\mathfrak{p}) \setminus \{0\}$) andiamo in $K(R/\mathfrak{p})[X] = S^{-1}R/\mathfrak{p}[X]$. È facile vedere che le ipotesi implicano $\bar{\mathfrak{q}}_2 \cap S = \bar{\mathfrak{q}}_3 \cap S = \emptyset$, per cui per la nota corrispondenza fra ideali negli anelli di frazioni abbiamo una catena

$$0 \subsetneq S^{-1}\bar{\mathfrak{q}}_2 \subsetneq S^{-1}\bar{\mathfrak{q}}_3$$

Questo è assurdo perché $K(R/\mathfrak{p})[X]$ ha dimensione 1 (è un PID).

2. Supponiamo di avere in $R[X]$ una catena

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_{2d+2}$$

Per il punto precedente quando la contraiamo ad R dovremmo ottenere una catena lunga almeno $d + 1$. □

L'Esercizio precedente è il meglio che si può fare, nel senso che c'è gente che si è messa lì e ha trovato esempi dove viene qualunque cosa fra $d + 1$ e $2d + 1$; si veda [17]. Aggiungendo l'ipotesi che R sia noetheriano la situazione cambia drasticamente: chiudiamo in bellezza il Capitolo (e la parte di Algebra Commutativa) mostrando che se R è noetheriano allora $\dim_{\text{Krull}}(R[X]) = \dim(R)+1$. Nel dimostrarlo faremo uso di un risultato che prende il nome di Teorema della Dimensione della Fibra, a cui ci incominciamo ad avvicinare spiegandone il nome. Sia $f\colon R \to R'$ un omomorfismo di anelli noetheriani e consideriamo $f^{\#}\colon \operatorname{Spec}(R') \to \operatorname{Spec} R$ definita come $\mathfrak{p} \mapsto \mathfrak{p}^c$. Su $\operatorname{Spec}(R)$ mettiamo l'usuale topologia dove i chiusi sono, al variare di $E \subseteq R$ sottoinsieme[27],

$$V(E) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq E\}$$

La "fibra" nel nome del Teorema è quella della mappa $f^{\#}$ fra questi spazi topologici. A noi comunque interessa più il lato algebrico delle cose.

[27] Senza nessuna struttura aggiuntiva.

Teorema 5.31 (della Dimensione della Fibra)**.** Siano R, R' locali noetheriani con ideali massimali $\mathfrak{m}$ ed $\mathfrak{m}'$. Supponiamo inoltre che $f\colon R \to R'$ sia *locale*, cioè $f(\mathfrak{m}) \subseteq \mathfrak{m}'$. Allora

$$\dim R' \leq \dim R + \dim {}^{R'}\!/_{\mathfrak{m}R'}$$

Se inoltre f è *piatta*, cioè se R' è un $f(R)$-modulo piatto[28], vale l'uguaglianza.

Cosa c'entra questo con la fibra? Il punto è che $\dim \operatorname{Spec} R = \dim_{\text{Krull}} R$. Guardando le mappe fra gli Spec introdotte prima ci si convince abbastanza in fretta che le fibre sono moralmente $R'/\mathfrak{m}R'$, quindi quello che il Teorema sta dicendo è che la dimensione in partenza è la dimensione in arrivo più la dimensione della fibra nel punto $\mathfrak{m}$. Prima di tuffarci nella dimostrazione ricordiamo che $R'/\mathfrak{m}R' \cong R' \otimes_R R/\mathfrak{m}$ (e quindi la parola "piatto" non appare a caso) secondo la mappa $r' \otimes [r] \mapsto [rr']$.

Dimostrazione. Per dimostrare la prima parte è sufficiente esibire[29] $\dim R + \dim R'/\mathfrak{m}R' = a + b$ elementi che generano un ideale $\mathfrak{m}'$-primario di R', perché allora $a + b \geq \delta(R') = \dim(R')$. Per il Teorema della Dimensione esistono $x_1, \dots, x_a \in \mathfrak{m}$ che generano un ideale $\mathfrak{m}$-primario $\mathfrak{q} = (x_1, \dots, x_a)$ di R. Prendiamo la proiezione al quoziente $\varphi\colon R'/\mathfrak{q}R' \to R'/\mathfrak{m}R'$ e notiamo che $\operatorname{Ker}\varphi$ è nilpotente perché lo possiamo scrivere come $\mathfrak{m}R'/\mathfrak{q}R'$ e siccome siamo in un anello noetheriano esiste n tale che $\mathfrak{m}^n \subseteq \mathfrak{q}$. Ma allora $\dim R'/\mathfrak{q}R' = \dim R'/\mathfrak{m}R' = b$, perché un ideale nilpotente è incluso nel nilradicale, cioè nell'intersezione di tutti i primi, e quindi è "invisibile" alla dimensione di Krull[30]. Possiamo allora trovare, usando di nuovo il Teorema della Dimensione, $y_1, \dots, y_b \in \mathfrak{m}'/\mathfrak{q}R'$ tali che $J = (y_1, \dots, y_b)$ sia $\mathfrak{m}'/\mathfrak{q}R'$-primario. Sia $\check{J} \subseteq R'$ la contrazione di J secondo la proiezione $R' \to R'/\mathfrak{q}R'$. L'ideale $\check{J}$ è $\mathfrak{m}'$-primario ed è generato da[31] $\check{y}_1, \dots, \check{y}_b, x_1, \dots, x_a$, e quindi è proprio quello che cercavamo.

Proviamo ora a mostrare l'altra disuguaglianza, cioè $\dim R' \geq a + b$, e vediamo dove ci blocchiamo[32]. Prendiamo una catena di primi in $R'/\mathfrak{m}R'$

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_b$$

[28] Nozione che dovrebbe essere stata definita ad Algebra 2, ma che comunque richiameremo nella Definizione 6.11.

[29] Ad essere completamente formali dovremmo scrivere $f(\mathfrak{m})R'$ invece di $\mathfrak{m}R'$ (anche nell'enunciato del Teorema), ma evitiamo di appesantire troppo la notazione.

[30] La teoria della dimensione è fatta apposta per poter quozientare per ideali nilpotenti senza pensieri. Addirittura se uno prende un approccio assiomatico alla dimensione, che poi verrà fuori partorire la dimensione che stiamo usando, una delle richieste ragionevoli da fare negli assiomi è proprio questa. La cosa viene fuori anche da necessità della geometria algebrica per ovvi motivi.

[31] Anche qui $x_1, \dots, x_a$ dovrebbero essere $f(x_1), \dots, f(x_a)$, ma ho preferito che l'abuso di notazione rimanesse coerente.

[32] Nell'enunciato l'uguaglianza è vera sotto l'ipotesi aggiuntiva di piattezza.

e solleviamola ad R'

$$\mathfrak{m}R' \subseteq \check{\mathfrak{q}}_0 \subsetneq \check{\mathfrak{q}}_1 \subsetneq \ldots \subsetneq \check{\mathfrak{q}}_b$$

Ora $f^{-1}(\check{\mathfrak{q}}_0) = \mathfrak{m}$, perché $\mathfrak{m} \subseteq f^{-1}(\check{\mathfrak{q}}_0)$ ed $\mathfrak{m}$ è massimale[33]. Quello che vorremmo fare adesso è prendere in R una catena di a primi

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_a = f^{-1}(\check{\mathfrak{q}_0}) = \mathfrak{m}$$

e sollevarla per completare la catena di prima ad una di lunghezza $a + b$ in R'. Per concludere ci serve dunque una sorta di Going Down, ed è qui che entra in gioco la piattezza. La dimostrazione è dunque conclusa a patto di avere il Teorema seguente. □

Teorema 5.32 (Going Down, caso piatto)**.** Sia $f\colon R \to R'$ una mappa piatta di anelli noetheriani, e siano $\mathfrak{q}$ primo di R' e $\mathfrak{p} \supsetneq \mathfrak{p}_0$ primi di R tali che $\mathfrak{q}^c = \mathfrak{p}$. Allora esiste un primo $\mathfrak{q}_0 \subsetneq \mathfrak{q}$ di R' tale che $\mathfrak{q}_0^c = \mathfrak{p}_0$.

Dimostrazione. Useremo (e giustificheremo in seguito) che

1. La mappa $R \to R' \to R'_{\mathfrak{q}}$ è ancora piatta. Dunque possiamo lavorare in $R'_{\mathfrak{q}}$, a meno di contrarre il $\mathfrak{q}_0$ di $R'_{\mathfrak{q}}$ a un $\tilde{\mathfrak{q}}_0$ di R'.
2. La mappa $R/\mathfrak{p}_0 \to R'/(\mathfrak{p}_0 R')$ è ancora piatta.

Possiamo dunque supporre che $\mathfrak{p}_0 = (0)$ (e dunque che R sia un dominio), $f\colon R \to R'$ con R' locale e $\mathfrak{q}$ massimale, $\mathfrak{q}^c = \mathfrak{p}$ e $\mathfrak{p} \supsetneq \mathfrak{p}_0 = (0)$. Cerchiamo quindi $\mathfrak{q}_0$ in R' tale che $\mathfrak{q}_0 \cap R = (0)$. Qualunque $\mathfrak{q}_0$ primo minimale[34] di R' andrà bene per lo scopo: infatti se fosse $\mathfrak{q}_0^c = \mathfrak{q}_0 \cap R \neq (0)$, sia $x \in \mathfrak{q}_0^c \setminus \{0\}$. Dato che R è un dominio, la successione $0 \to R \xrightarrow{\cdot x} R$ è esatta, e usando la piattezza otteneniamo la successione esatta

$$0 \to R \otimes_R R' \xrightarrow{\cdot x \otimes \mathrm{id}} R \otimes_R R'$$

Inoltre $R \otimes_R R'$ è in maniera ovvia isomorfo ad R' e la mappa $\cdot x \otimes \mathrm{id}$ diventa $f(x)$ perché $x \otimes 1 = 1 \otimes f(x)$. Abbiamo dunque la successione esatta

$$0 \to R' \xrightarrow{\cdot f(x)} R'$$

Ma questo è assurdo perché $\cdot f(x)$ non può essere iniettiva: infatti dato che R' è noetheriano (0) ammette decomposizione primaria, e i divisori di 0 sono l'unione dei primi minimali di (0). Ne segue che gli elementi di $\mathfrak{q}_0$, e in particolare $f(x)$ perché $x \in \mathfrak{q}_0^c \setminus \{0\}$, sono tutti divisori di 0. Occupiamoci ora delle ipotesi assunte all'inizio:

[33] $f^{-1}(\check{\mathfrak{q}}_0)$ è proprio perché gli omomorfismi mandano 1 in 1.

[34] Ne esiste almeno uno per decomposizione primaria, per la quale si rimanda come sempre a [2], Proposizione 4.6 e Teorema 7.13.

1. Che la composizione $R \to R' \to R'_{\mathfrak{q}}$ sia piatta si vede ricordandosi che per ogni R'-modulo K vale $S^{-1}K \cong S^{-1}R' \otimes_{R'} K$ e scrivendo la sequenza di successioni esatte

$$\begin{array}{ll} 0 \to N \to M & \\ 0 \to R' \otimes_R N \to R' \otimes_R M & (f \text{ piatta}) \\ 0 \to R'_{\mathfrak{q}} \otimes_{R'} R' \otimes_R N \to R'_{\mathfrak{q}} \otimes_{R'} R' \otimes_R M & (S^{-1} \text{ esatta}) \\ 0 \to R'_{\mathfrak{q}} \otimes_R N \to R'_{\mathfrak{q}} \otimes_R M & (R'_{\mathfrak{q}} \otimes_{R'} R' \cong R'_{\mathfrak{q}}) \end{array}$$

2. Usando il Lemma seguente con $S = R/\mathfrak{p}_0$ e scrivendo $R'/(\mathfrak{p}_0 R') \cong R/\mathfrak{p}_0 \otimes_R R'$. □

Lemma 5.33. Sia $R \to R'$ piatta e sia S una R-algebra. Allora $S \to S \otimes_R R'$ è piatta.

Dimostrazione. La tesi vuol dire che se $0 \to N \to M$ è una successione esatta di S-moduli allora anche

$$0 \to N \otimes_S (S \otimes_R R') \to M \otimes_S (S \otimes_R R') \tag{5.1}$$

è esatta. Sicuramente, dato che $M \cong M \otimes_S S$ abbiamo l'esattezza di

$$0 \to N \otimes_S S \to M \otimes_S S$$

Se la guardiamo come successione di R-moduli e tensorizziamo per R' otteniamo, grazie alla piattezza di $R \to R'$,

$$0 \to (N \otimes_S S) \otimes_R R' \to (M \otimes_S S) \otimes_R R'$$

e per associatività del prodotto tensore possiamo spostare le parentesi ottenendo l'esattezza della successione (5.1), che è la tesi. □

Teorema 5.34. Se R è noetheriano di dimensione finita la dimensione di $R[X]$ è $\dim R + 1$.

Dimostrazione. $\dim R[X] \geq \dim R + 1$ è facile: se

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

è una catena massimale di primi in R, basta considerare

$$\mathfrak{p}_0 R[X] \subsetneq \mathfrak{p}_1 R[X] \subsetneq \ldots \subsetneq \mathfrak{p}_n R[X] \subsetneq (X, \mathfrak{p}_n) R[X]$$

Che le inclusioni rimangano strette è facile da verificare. Inoltre i $\mathfrak{p}_i R[X]$ sono primi perché $R[X]/\mathfrak{p}_i R[X] \cong (R/\mathfrak{p}_i)[X]$, e $(X, \mathfrak{p}_n)R[X]$ è primo perché il quoziente è $R/\mathfrak{p}_n$. Occupiamoci ora della disuguaglianza difficile. Sia

$$\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_m \subsetneq R[X]$$

una catena di primi e poniamo $\mathfrak{p} = \mathfrak{q}_m \cap R$. Notiamo anche che c'è un'immersione γ

$$0 \to R_{\mathfrak{p}} \xrightarrow{\gamma} R[X]_{\mathfrak{q}_m}$$

e che γ è una mappa locale, cioè[35] $\gamma(\mathfrak{p}^e) \subseteq \mathfrak{q}_m^e$. In $R[X]_{\mathfrak{q}_m}$ abbiamo la catena

$$\mathfrak{q}_0^e \subsetneq \ldots \subsetneq \mathfrak{q}_m^e$$

e quindi, usando questa catena e il Teorema della Dimensione della Fibra,

$$m \leq \dim R[X]_{\mathfrak{q}_m} \leq \dim R_{\mathfrak{p}} + \dim \underbrace{R[X]_{\mathfrak{q}_m} \big/ \mathfrak{p} R[X]_{\mathfrak{q}_m}}_{=B}$$

Dunque, dato che $\dim R_{\mathfrak{p}} \leq \dim R$, è sufficiente provare che $\dim B \leq 1$. Per mostrare ciò basta trovare un campo $\mathbb{K}$ che ci permetta di "incastrare" B:

$$\mathbb{K}[X] \subseteq B \subseteq \mathbb{K}(X)$$

Infatti, se riusciamo a mostrare questo, allora B è un anello di frazioni di $\mathbb{K}[X]$ e dunque $\dim B \leq 1$, perché possiamo porre

$$S = \left\{ f \in \mathbb{K}[X] \;\middle|\; \frac{1}{f} \in B \right\}$$

e verificare che $S^{-1}\mathbb{K}[X] = B$. L'inclusione $\subseteq$ è ovvia, e viceversa dato un qualunque $g/h \in B$, con g, h coprimi, per mostrare che $h \in S$ basta notare che per Bézout esistono $\lambda, \mu \in \mathbb{K}[X]$ tali che $\lambda g + \mu h = 1$, e dunque

$$\frac{1}{h} = \lambda \frac{g}{h} + \mu \frac{h}{h} \in B$$

Come $\mathbb{K}$ possiamo prendere il campo residuo di $R_{\mathfrak{p}}$. Infatti componendo l'immersione $R_{\mathfrak{p}}[X] \hookrightarrow R[X]_{\mathfrak{q}_m}$ con la proiezione al quoziente su B otteniamo

$$\varphi \colon R_{\mathfrak{p}}[X] \to R[X]_{\mathfrak{q}_m} \big/ \mathfrak{p} R[X]_{\mathfrak{q}_m} = B$$

Dato che $\mathfrak{p} = \mathfrak{q}_m \cap R$ abbiamo $\operatorname{Ker} \varphi = \mathfrak{p} R_{\mathfrak{p}}[X]$, da cui l'inclusione

$$R_{\mathfrak{p}} \big/ \mathfrak{p} R_{\mathfrak{p}}[X] = \mathbb{K}[X] \hookrightarrow B$$

Ora consideriamo la mappa

$$\vartheta \colon R[X]_{\mathfrak{q}_m} \to \left(R_{\mathfrak{p}} \big/ \mathfrak{p} R_{\mathfrak{p}} \right)(X) \qquad \vartheta\left(\frac{f}{g}\right) = \frac{\bar{f}}{\bar{g}}$$

la cui buona definizione si ottiene combinando $g \notin \mathfrak{q}_m$ con $\mathfrak{p} = \mathfrak{q}_m \cap R$. Dato che $\operatorname{Ker} \vartheta = \mathfrak{p} R[X]_{\mathfrak{q}_m}$ otteniamo l'inclusione

$$R[X]_{\mathfrak{q}_m} \big/ \mathfrak{p} R[X]_{\mathfrak{q}_m} = B \hookrightarrow \mathbb{K}(X) \qquad \square$$

[35] Le estensioni si intendono secondo la mappa S^{-1}.

Grazie a questo Teorema è immediato dire che, ad esempio, $\dim \mathbb{Z}[X,Y] = 3$.

Esercizio 5.35. Sia $A = \mathbb{Z}[X,Y]$ e $I = (X^2 - XY + X, XY - Y^2 + Y)$. Calcolare $\dim A/I$.

Soluzione. Una catena di primi in A/I lunga m si solleva ad una lunga $m+1$ in A aggiungendoci (0). Da ciò segue $m + 1 \leq 3$, e quindi $\dim A/I \leq 2$. Inoltre possiamo scrivere

$$I = (X(X - Y + 1), Y(X - Y + 1))$$

e dunque (occhio: I non è primo), per ogni primo $p \in \mathbb{Z}$, abbiamo la catena

$$I \subsetneq (X - Y + 1) \subsetneq (X, Y - 1) \subsetneq (X, Y - 1, p)$$

che, quozientando, fornisce una catena di primi in A/I di lunghezza[36] 2. □

[36]Notare come la dimensione cali solo di 1 anche se I è generato da 2 elementi.

Parte II

Algebra Omologica

Capitolo 6

Introduzione

Il testo di riferimento per questa parte è [6], e un altro testo consigliato è di nuovo [5]. Appunti di un vecchio corso sono disponibili in [4] e [8]. L'obiettivo generale è arrivare a parlare di *funtori derivati* e studiare due signori conosciuti con i nomi di Ext^n e Tor_n, imparentati rispettivamente con estensioni di moduli e prodotto tensore.

D'ora in poi gli anelli non saranno sempre supposti commutativi, ma saranno comunque muniti di unità, con le dovute conseguenze sui morfismi, come spiegato all'inizio della parte precedente. In altre parole, se finora "anello" era un diminutivo per "anello commutativo con unità" adesso sta a significare "anello con unità". Invece che A o R un anello si chiamerà tendenzialmente Λ, e indicheremo con Λ^{op} l'anello ottenuto da Λ facendo la moltiplicazione al contrario. Formalmente, si "rietichettano" tutti gli elementi di Λ aggiungendoci un "op" ad apice

$$\Lambda^{\mathrm{op}} = \{\lambda^{\mathrm{op}} \mid \lambda \in \Lambda\}$$

e si definiscono le operazioni di Λ^{op} come[1]

$$\lambda_1^{\mathrm{op}} + \lambda_2^{\mathrm{op}} = (\lambda_1 + \lambda_2)^{\mathrm{op}}$$
$$\lambda_1^{\mathrm{op}} \lambda_2^{\mathrm{op}} = (\lambda_2 \lambda_1)^{\mathrm{op}}$$

Chiaramente se Λ è commutativo allora $\Lambda \cong \Lambda^{\mathrm{op}}$. Anche per i moduli bisogna cominciare a fare dei distinguo:

Definizione 6.1. Un Λ-*modulo sinistro* M è un Λ-modulo con la usuale definizione. Un Λ-*modulo destro* è un Λ^{op}-modulo sinistro.

Se diciamo "modulo" e basta intendiamo "modulo sinistro". Concretamente possiamo pensare alla (e scrivere la) moltiplicazione per scalare a

[1] Le operazioni a destra sono quelle di Λ.

destra invece che a sinistra, e quando si moltiplica per due elementi dell'anello l'ordine si scambia e dunque l'operazione coincide con quella di Λ^{op}. Per chiarirsi le idee, mentre nei moduli sinistri $\lambda_1 \cdot (\lambda_2 \cdot m) = (\lambda_1\lambda_2) \cdot m$,

$$(m \cdot \lambda_2) \cdot \lambda_1 = \lambda_1^{\mathrm{op}} \cdot (\lambda_2^{\mathrm{op}} \cdot m) = (\lambda_1^{\mathrm{op}}\lambda_2^{\mathrm{op}}) \cdot m = (\lambda_2\lambda_1)^{\mathrm{op}} \cdot m = m \cdot (\lambda_2\lambda_1)$$

Osservazione 6.2. L'insieme degli omomorfismi fra due fissati Λ-moduli[2] $\mathrm{Hom}_\Lambda(M, N)$ è in generale solo un gruppo abeliano, e non ha una struttura ovvia[3] di Λ-modulo come nel caso commutativo.

Il punto è che se uno prova a definire $\lambda\varphi$ come $\lambda\varphi(m) = \varphi(\lambda m)$ e scrive

$$\lambda(\mu\varphi(m)) = \mu\varphi(\lambda m) = \varphi((\mu\lambda)m) \stackrel{?}{=} \varphi((\lambda\mu)m) = (\lambda\mu)\varphi(m)$$

ha bisogno che Λ sia commutativo per togliere il punto interrogativo e avere l'associatività del prodotto per scalare.

6.1 Cosa Sappiamo Già

In questa sezione ricapitoliamo un po' di risultati noti da Algebra 2, dove probabilmente gli anelli commutavano, ma le dimostrazioni funzionano lo stesso. Il lettore scettico può fare riferimento a [6], principalmente nel Capitolo I.

Proposizione 6.3. Siano $0 \to B' \xrightarrow{\mu} B \xrightarrow{\epsilon} B''$ una successione esatta di Λ-moduli e A un Λ-modulo. Allora la successione[4]

$$0 \to \mathrm{Hom}(A, B') \xrightarrow{\mu_*} \mathrm{Hom}(A, B) \xrightarrow{\epsilon_*} \mathrm{Hom}(A, B'')$$

è esatta, dove $\mu_* \colon \varphi \mapsto \mu \circ \varphi$ e similmente per ϵ.

Proposizione 6.4. Sia $B' \xrightarrow{\mu} B \xrightarrow{\epsilon} B'' \to 0$ una successione esatta di Λ-moduli e sia A un Λ-modulo. Allora la successione

$$0 \to \mathrm{Hom}(B'', A) \xrightarrow{\epsilon^*} \mathrm{Hom}(B, A) \xrightarrow{\mu^*} \mathrm{Hom}(B', A)$$

è esatta, dove questa volta[5] $\mu^* \colon \varphi \mapsto \varphi \circ \mu$, e similmente per ϵ^*.

I *funtori*[6] $\mathrm{Hom}(A, -)$ e $\mathrm{Hom}(-, A)$ si dicono *esatti a sinistra*, perché portano successioni esatte a destra/sinistra (a seconda del fatto che "girino le frecce"

[2] Se Λ è chiaro dal contesto scriveremo anche solo $\mathrm{Hom}(M, N)$.

[3] Qualcuno direbbe "naturale".

[4] Di gruppi abeliani, per quanto detto poco fa. D'ora in avanti eviteremo di continuare a puntualizzare questa cosa.

[5] *NdA*: come trucco mnemonico io uso "buco a sinistra – buco a sinistra, buco a destra – buco a destra", nel senso che il "buco" a destra in $\mathrm{Hom}(A, -)$ è associato al "buco" (lo 0 che non c'è) a destra nella successione esatta $0 \to B' \to B \to B''$, eccetera. Per ricordarsi se $*$ va in alto o in basso, sempre in dipendenza dalla posizione del "buco", penso a quale pugno alzato costituisce un gesto politico.

[6] Spiegheremo nella Sezione 6.4 il significato del termine.

o meno) in successioni esatte a sinistra (conta la successione in arrivo). Le altre esattezze si possono perdere: ad esempio se prendiamo la successione esatta di $\mathbb{Z}$-moduli (gruppi abeliani)

$$0 \to \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

e poniamo $A = \mathbb{Z}/n\mathbb{Z}$ allora la successione qui sotto rimane esatta

$$0 \to \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}\right) \xrightarrow{(n\cdot)_*} \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}\right) \xrightarrow{\pi_*} \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\right)$$

ma per $|n| > 1$ la mappa π_* non è surgettiva, cosa di cui ci si accorge subito notando che il gruppo in partenza è quello banale e quello in arrivo no. Per mostrare un controesempio per l'altro caso è sufficiente considerare la stessa successione, sempre con $|n| > 1$, e usare $A = \mathbb{Z}$:

$$0 \to \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}\right) \xrightarrow{\pi^*} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{(n\cdot)^*} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$$

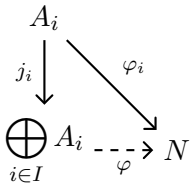
Qui $(n\cdot)^*$ non è surgettiva perché ad esempio non acchiappa l'identità $\mathbb{Z} \to \mathbb{Z}$. Infatti, supponendo $\mathrm{id} = \big((n\cdot)^*(f)\big)$, abbiamo

$$1 = \mathrm{id}(1) = \big((n\cdot)^*(f)\big)(1) = \big(f \circ (n\cdot)\big)(1) = f(n \cdot 1) = n \cdot f(1)$$

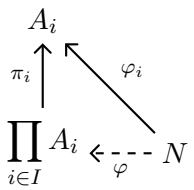
dunque $\mathbb{Z} \ni f(1) = 1/n$, ma dato che $|n| > 1$ questo è assurdo.

Definizione 6.5. Sia $(A_i)_{i\in I}$ una famiglia di Λ-moduli.

- Un Λ-modulo M si dice *somma diretta* degli $(A_i)_{i\in I}$ (e si scrive $M = \bigoplus_{i\in I} A_i$) se esistono degli omomorfismi "di inclusione" $j_i \colon A_i \to M$ tali che per ogni Λ-modulo N e omomorfismi $\{\varphi_i \colon A_i \to N \mid i \in I\}$ esiste un unico φ che fa commutare, al variare di $i \in I$, tutti i



- Il *prodotto diretto* si definisce in maniera analoga ma con tutte le frecce al contrario, e con le "proiezioni" invece che le "inclusioni". Dunque i diagrammi che devono commutare sono



Queste definizioni vanno bene in contesti molto generali (ossia categorie, vedi Sezione 6.4), nei quali si può mostrare che somma e prodotto diretto sono unici a meno di isomorfismo. Comunque nel caso dei moduli somma e prodotto diretto sono quelli che già conosciamo.

Proposizione 6.6. Sia B un Λ-modulo e $(A_j)_{j\in J}$ una famiglia di Λ-moduli. Allora

$$\mathrm{Hom}_\Lambda\Big(\bigoplus_{j\in J} A_j, B\Big) \cong \prod_{j\in J} \mathrm{Hom}_\Lambda(A_j, B)$$

Idea della Dimostrazione. Da un omomorfismo $\bigoplus A_j \to B$ si ricavano tanti omomorfismi $A_j \to B$, e si verifica che la prima mappa sensata che ci viene in mente funziona. □

Per quanto sopra, ponendo $A_j = B = \mathbb{R}$ si ha che

$$\Big(\bigoplus_{i=0}^{\infty} \mathbb{R}\Big)^* = \prod_{i=0}^{\infty} \mathbb{R}$$

o, in altre parole,

Corollario 6.7. Il duale dei polinomi sono le serie.

Lemma 6.8 (del Serpente)**.** Se il seguente diagramma commuta ed ha le righe esatte

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\xi} & B & \xrightarrow{\eta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[\varphi]{} & B' & \xrightarrow[\psi]{} & C' & & \end{array}$$

allora esiste d che rende la seguente successione esatta[7]

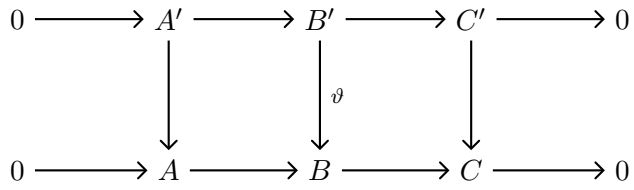
$$\mathrm{Ker}\,\alpha \xrightarrow{\xi_\restriction} \mathrm{Ker}\,\beta \xrightarrow{\eta_\restriction} \mathrm{Ker}\,\gamma \xrightarrow{d} \mathrm{Coker}\,\alpha \xrightarrow{\overline{\varphi}} \mathrm{Coker}\,\beta \xrightarrow{\overline{\psi}} \mathrm{Coker}\,\gamma$$

inoltre se ξ è iniettiva anche $\xi_\restriction$ lo è, e se ψ è surgettiva anche $\overline{\psi}$ lo è[8].

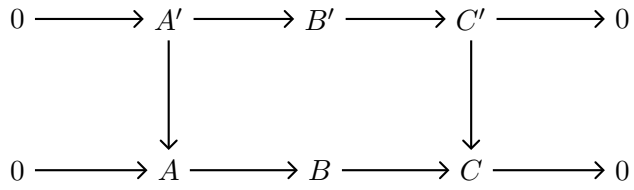
Proposizione 6.9. Nei diagrammi commutativi a righe esatte come quello qui sotto, se le frecce verticali ai lati sono isomorfismi anche ϑ lo è.

[7] $\xi_\restriction$ indica la restrizione di ξ e $\overline{\varphi}$ indica la mappa indotta da φ al quoziente. Similmente per η e ψ.

[8] In altre parole se c'è uno 0 in più in alto a sinistra nel diagramma c'è uno 0 in più a sinistra nella successione esatta, e se c'è uno 0 in più in basso a destra c'è uno 0 in più a destra.



Occhio: *se ϑ esiste* e fa commutare tutto è un isomorfismo. In generale in una situazione del tipo



con le frecce verticali isomorfismi, si può avere $A \cong A'$, $C \cong C'$ ma $B \ncong B'$. Questo sarà palese quando, nella Sezione 7.4, parleremo di estensioni di moduli, ma anche ora non sarebbe difficile fabbricare un controesempio, ad esempio con $\mathbb{Z}/4\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ come B e B' (cfr. Esempio 6.21).

Proposizione 6.10. Siano $B' \xrightarrow{\mu} B \xrightarrow{\epsilon} B'' \to 0$ una successione esatta di Λ-moduli sinistri e A un Λ-modulo destro[9]. Allora è esatta anche

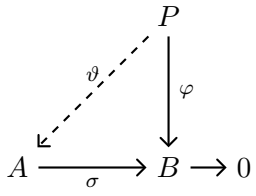
$$A \otimes_\Lambda B' \xrightarrow{\mathrm{id}\otimes\mu} A \otimes_\Lambda B \xrightarrow{\mathrm{id}\otimes\epsilon} A \otimes_\Lambda B'' \to 0$$

Dunque, se gli Hom_Λ erano esatti *a sinistra*, diciamo che $A \otimes_\Lambda -$ è *esatto a destra*. Lo stesso risultato vale per[10] $- \otimes_\Lambda B$.

Definizione 6.11. Un Λ-modulo A si dice *piatto* se per ogni successione esatta $0 \to B' \xrightarrow{\mu} B \xrightarrow{\epsilon} B'' \to 0$ di Λ moduli è esatta anche la successione

$$0 \to A \otimes_\Lambda B' \xrightarrow{\mathrm{id}\otimes\mu} A \otimes_\Lambda B \xrightarrow{\mathrm{id}\otimes\epsilon} A \otimes_\Lambda B'' \to 0$$

Definizione 6.12. Un modulo P si dice *proiettivo*[11] se per ogni scelta di A, B, σ, φ come nel diagramma[12] esiste ϑ che lo fa commutare.



[9] Per far funzionare il prodotto tensore $A \otimes_\Lambda B$ serve che A sia destro e B sinistro. In generale su $A \otimes_\Lambda B$ si ha solo una struttura di gruppo abeliano.

[10] Che però prende "in input" moduli destri.

[11] Il lettore curioso di sapere da dove viene il termine "proiettivo" dia un'occhiata alla presentazione dei moduli proiettivi in [3]. Non indico sezione né numero di pagina perché mi sembra che siano ancora in fieri.

[12] La "$\to 0$" sta ad indicare che $\sigma\colon A \to B$ è surgettiva, che è una notazione comoda perché quando fra poco gireremo tutte le frecce...

In altre parole i moduli proiettivi sono quelli dove ogni fattorizzazione sensata[13] di una mappa uscente è possibile, o dove "quando si esce si può allungare il giro". Detto in un'altra maniera ancora, le mappe a valori in un quoziente $B = A/(\dots)$ possono essere sollevate ad A.

Proposizione 6.13. Ogni modulo libero è proiettivo.

Proposizione 6.14. $\bigoplus_{i \in I} A_i$ è proiettivo se e solo se ogni A_i è proiettivo.

Proposizione 6.15. Sia $0 \to A \xrightarrow{\mu} B \xrightarrow{\epsilon} C \to 0$ esatta. Se esiste $\sigma\colon C \to B$ tale che $\epsilon \circ \sigma = \mathrm{id}_C$ allora la successione *spezza*, ovvero esiste ϑ tale che[14]

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{i_A} & A \oplus C & \xrightarrow{\pi_C} & C & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \vartheta} & & \| & & \\
0 & \longrightarrow & A & \xrightarrow[\mu]{} & B & \xrightarrow[\epsilon]{} & C & \longrightarrow & 0
\end{array}$$

e lo stesso risultato vale se esiste $\gamma\colon B \to A$ tale che $\gamma \circ \mu = \mathrm{id}_A$.

Teorema 6.16 (di Caratterizzazione dei Moduli Proiettivi)**.** Sia P un Λ-modulo. Sono equivalenti

1. P è proiettivo.
2. Per ogni successione esatta $0 \to A \to B \to C \to 0$ la successione
$$0 \to \mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B) \to \mathrm{Hom}(P, C) \to 0$$
è esatta.
3. Se $\epsilon\colon B \to P \to 0$ allora esiste $\sigma\colon P \to B$ tale che $\epsilon \circ \sigma = \mathrm{id}_P$.
4. P è addendo diretto di ogni modulo di cui è quoziente.
5. P è addendo diretto di un modulo libero.

Proposizione 6.17. Ogni modulo proiettivo è anche piatto.

Proposizione 6.18. Se Λ è un PID[15] ogni Λ-modulo è proiettivo se e solo se è libero.

[13] Se σ non è surgettiva, ad esempio se mappa tutto in 0, è facile trovare φ che non ammettono nessuna ϑ.

[14] Spesso diremo "tale che [diagramma]" intendendo che il diagramma commuti. Analogamente le righe con degli 0 hanno la tendenza ad essere esatte (ma a volte no; dovrebbe essere chiaro dal contesto). Le doppie righe verticali sarebbero un "=" allungato, e ovviamente indicano l'identità.

[15] Qui uno potrebbe chiedersi quali sono gli ideali che devono essere principali (destri? sinistri? bilateri?), ma "commutativo" è inteso gratis nella definizione di PID, addirittura di dominio.

Per anelli a caso non è più vero:

Esempio 6.19. Consideriamo la successione esatta di $\mathbb{Z}/p^2\mathbb{Z}$-moduli[16]

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{[1]_p \mapsto [p]_{p^2}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{[m]_{p^2} \mapsto [m]_p} \mathbb{Z}/p\mathbb{Z} \to 0$$

Se $\mathbb{Z}/p\mathbb{Z}$ fosse uno $\mathbb{Z}/p^2\mathbb{Z}$-modulo proiettivo questa, per i risultati richiamati poco fa, spezzerebbe e avremmo l'assurdo $\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Esempio 6.20. Sia $\Lambda = \mathbb{Z}/12\mathbb{Z}$. Consideriamo l'isomorfismo

$$(\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}) \xrightarrow{([a]_3,[b]_4) \mapsto [4a+3b]_{12}} \mathbb{Z}/12\mathbb{Z}$$

Λ è un Λ-modulo libero, e quindi proiettivo, e $\mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/4\mathbb{Z}$ sono Λ-moduli proiettivi in quanto addendi diretti di un libero, ma non sono liberi: ad esempio ogni elemento x di $\mathbb{Z}/3\mathbb{Z}$ soddisfa $[3]_{12} \cdot x = 0$, e quindi $\mathbb{Z}/3\mathbb{Z}$ non ha sottoinsiemi indipendenti di cardinalità 1.

Esempio 6.21. In $\mathbb{Z}/4\mathbb{Z}$ l'unico sottomodulo non banale è $2\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, che non è proiettivo, altrimenti da

$$0 \to 2\mathbb{Z}/4\mathbb{Z} \xrightarrow{[m]_4 \mapsto [m]_4} \mathbb{Z}/4\mathbb{Z} \xrightarrow{[m]_4 \mapsto [m]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

avremmo l'assurdo $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Esercizio 6.22 (Sfida)**.** Lo $\mathbb{Z}$-modulo $\prod_{n\in\mathbb{N}} \mathbb{Z}$ non è libero[17].

Una soluzione è reperibile in [16].

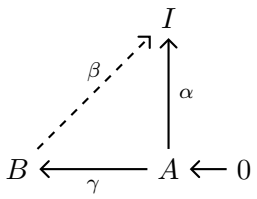
6.2 Moduli Iniettivi

I moduli iniettivi funzionano come i proiettivi, ma "a rovescio": ogni fattorizzazione sensata di una mappa entrante è possibile, o "quando si entra si può allungare il giro". Come anticipato "0 $\to$" sta ad indicare che $\gamma\colon A \to B$ è iniettiva, che è la condizione di "sensatezza" per motivi analoghi (o meglio, duali) a prima: se ad esempio γ manda tutto in 0... Per una motivazione più rigorosa del fatto che "iniettivo" sia "surgettivo a frecce girate" guardare la presentazione dei moduli iniettivi su [6], Sezione 6 del Capitolo I.

Definizione 6.23. Un modulo I si dice *iniettivo* se per ogni scelta di A, B, α, γ come nel diagramma esiste β che lo fa commutare.

[16] Anche questa volta la moltiplicazione per scalare è la prima sensata che vi viene in mente. Se non vi viene in mente provate scriverla (questa frase sembra non avere senso, ma a volte funziona).

[17] E quindi neppure proiettivo, dato che $\mathbb{Z}$ è un PID.



In questo caso dunque le mappe che partono da un sottomodulo di B a valori in I possono essere estese a tutto B. Dato che abbiamo girato le frecce nella definizione uno si potrebbe aspettare che girando le frecce nelle dimostrazioni si dimostrino i risultati enunciati prima per i moduli proiettivi, ma con le frecce girate. Funziona? Più o meno:

- Non è sempre immediatissimo capire cosa vuol dire girare le frecce, nemmeno negli enunciati. Cosa vuol dire girare le frecce in "A è un modulo libero"?[18]
- Anche se si girano le frecce degli enunciati non è detto che girare le frecce nelle dimostrazioni funzioni.

Per una discussione più completa in merito si veda sempre [6], all'inizio della Sezione 6 del Capitolo I. Comunque un esempio di cosa che si riesce veramente a dimostrare "girando le frecce" è il fatto che

Proposizione 6.24. $\prod_{j\in J} A_j$ è iniettivo se solo se ogni A_j è iniettivo.

Iniziamo a studiare la questione nei casi semplici: sui PID dire "proiettivo" o "libero" è la stessa cosa. Cosa succede per i moduli iniettivi?

Definizione 6.25. Sia Λ un dominio[19]. Un Λ-modulo D si dice *divisibile* se per ogni $d \in D$ e $\lambda \in \Lambda \setminus \{0\}$ esiste $c \in D$ tale che $\lambda c = d$.

Esempio 6.26. Lo $\mathbb{Z}$-modulo (gruppo abeliano) $\mathbb{Q}/\mathbb{Z}$ è divisibile, mentre $\mathbb{Z}$ no. Anche $\mathbb{Q}$ è divisibile. La differenza con $\mathbb{Q}/\mathbb{Z}$ è che per $\mathbb{Q}$ il c è unico, mentre in $\mathbb{Q}/\mathbb{Z}$ non è detto. Ad esempio se $d = [0]$ e $\lambda = 4$, come c vanno bene sia $[1/2]$ che $[1/4]$.

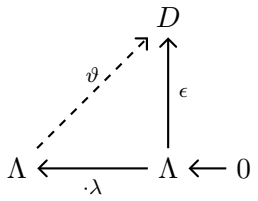
L'esempio non è a caso, $\mathbb{Q}/\mathbb{Z}$ lo rincontreremo fra poco.

Teorema 6.27. Se Λ è un dominio ogni Λ-modulo iniettivo è divisibile. Se Λ è un PID ogni Λ-modulo divisibile è iniettivo.

[18] Il lettore che ha già un po' di familiarità con le categorie e ha sentito parlare di funtori aggiunti potrebbe essersi imbattuto in qualcosa del tipo "un modulo libero è un modulo nell'immagine essenziale dell'aggiunto sinistro del funtore dimenticante in Set". Il funtore dimenticante in Set non ha un aggiunto destro (non preserva i coprodotti), ma non tutto è perduto. Si veda la nota 23 fra qualche pagina.

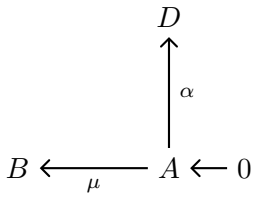
[19] In particolare Λ si suppone commutativo.

Dimostrazione. Siano Λ un dominio, D un Λ-modulo iniettivo, $d \in D$ e $\lambda \in \Lambda \setminus \{0\}$. Dobbiamo esibire c tale che $\lambda c = d$. Consideriamo il diagramma



dove $\epsilon(1) = d$ e l'iniettività di $\cdot\lambda$ segue dal fatto che Λ è un dominio. Per commutatività $\epsilon(1) = \vartheta(\lambda \cdot 1) = \lambda\vartheta(1)$, e dunque basta porre $c = \vartheta(1)$.

Sia ora Λ un PID e D divisibile. Vogliamo completare il diagramma



A meno di identificare A con $\mu(A)$ possiamo pensare $A \subseteq B$. Consideriamo

$$\Sigma = \{(L, \gamma) \mid A \subseteq L \subseteq B \text{ e } \gamma \colon L \to D, \gamma_{\restriction A} = \alpha\}$$

che è non vuoto perché contiene (A, α). Sia per Zorn $(\bar{A}, \bar{\alpha})$ massimale[20]. Supponiamo per assurdo $\bar{A} \neq B$ e sia $b \in B \setminus \bar{A}$. Prendiamo poi $\tilde{A} = \langle \bar{A}, b \rangle_\Lambda$ e vediamo che riusciamo ad estendere $\bar{\alpha}$ ad $\tilde{\alpha}$, contro la massimalità. Quello che vorremmo fare è definire $\tilde{\alpha} \colon \tilde{A} \to D$ come

$$\tilde{\alpha}(\bar{a} + \lambda b) = \bar{\alpha}(\bar{a}) + \lambda(?)$$

mettendo al posto di "(?)" qualcosa che la renda una buona definizione, cioè che non la faccia dipendere da $\bar{a}$ e λ, ed è qui che entra in gioco la divisibilità. Consideriamo l'ideale di Λ

$$I = \{\lambda \in \Lambda \mid \lambda b \in \bar{A}\} = (\lambda_0) \quad \text{(perché } \Lambda \text{ è un PID)}$$

L'idea è che per i λb con $\lambda \in I$ la mappa $\bar{\alpha}$ è già definita, e vorremmo definire $\tilde{\alpha}(b)$ "tirando fuori" il λ. Precisamente, se $\lambda_0 \neq 0$, dato che D è divisibile, esiste $c \in D$ tale che $\lambda_0 c = \bar{\alpha}(\lambda_0 b)$, mentre se $\lambda_0 = 0$ prendiamo c qualunque[21]. Il candidato al posto di "(?)" è proprio c, che permette di "tirare fuori" λ_0 da $\bar{\alpha}(\lambda_0 b)$. Verifichiamo che effettivamente questo rende $\tilde{\alpha}$ ben definita: se $\bar{a}' + \lambda' b = \bar{a} + \lambda b$ allora

$$\underbrace{\bar{a}' - \bar{a}}_{\in \bar{A}} = (\lambda - \lambda')b$$

[20] L'ordinamento, come ci si aspetta, è $(L, \gamma) < (L', \gamma')$ sse $L \subseteq L'$ e $\gamma'_{\restriction L} = \gamma$.

[21] In questo caso per qualunque scelta di c è comunque vero che $\lambda_0 c = \bar{\alpha}(\lambda_0 b)$.

Dunque $(\lambda - \lambda')b \in \bar{A}$, e per definizione $(\lambda - \lambda') \in I$, per cui $\lambda - \lambda' = \lambda_2\lambda_0$. Ne segue che

$$\bar{\alpha}(\bar{a}' - \bar{a}) = \bar{\alpha}(\lambda_2\lambda_0 b) = \lambda_2\bar{\alpha}(\lambda_0 b) = \lambda_2\lambda_0 c = (\lambda - \lambda')c$$

che, guardando i termini agli estremi, vuol dire esattamente

$$\bar{\alpha}(\bar{a}') + \lambda' c = \bar{\alpha}(\bar{a}) + \lambda c \qquad \square$$

Ora vogliamo mostrare[22] il duale di "ogni modulo è quoziente di un modulo libero". Forti di quanto appena dimostrato, visto che per i PID "libero" equivale a "proiettivo", iniziamo a "girare le frecce" nel caso $\Lambda = \mathbb{Z}$:

Teorema 6.28. Ogni gruppo abeliano ($\mathbb{Z}$-modulo) può essere immerso in un gruppo abeliano divisibile ($\mathbb{Z}$-modulo iniettivo).

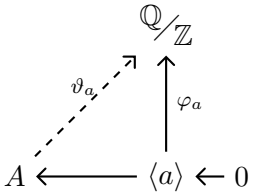
Dimostrazione. Iniziamo accontentandoci di immergere (il sottogruppo generato da) un elemento. Sia A uno $\mathbb{Z}$-modulo e sia $a \in A \setminus \{0\}$. Definiamo una mappa

$$\varphi_a \colon \langle a \rangle \to \mathbb{Q}/\mathbb{Z}$$

mandando a in

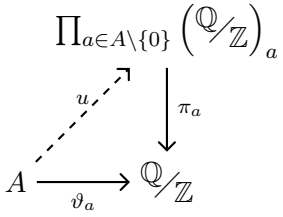
- Un qualunque elemento non nullo se a ha ordine infinito
- Se a ha ordine n, in un elemento di ordine che lo divide.

Poi estendiamo: per iniettività esiste ϑ_a che fa commutare



Se ora ϑ_a fosse iniettiva avremmo finito, ma nessuno ci assicura che questo succeda; sicuramente, però, $\vartheta_a(a) \neq 0$. Per avere una mappa in un modulo iniettivo veramente iniettiva ripetiamo la stessa costruzione per tutti gli $a \in A \setminus \{0\}$ e mettiamo insieme tutte le ϑ_a: visto che il prodotto di iniettivi è iniettivo, il prodotto di abbastanza copie di $\mathbb{Q}/\mathbb{Z}$ dovrebbe fare al caso nostro: in effetti, per la proprietà universale del prodotto diretto, esiste u che fa commutare tutti i diagrammi

[22] Ed enunciare, visto che come detto prima non è completamente ovvio.



e u è iniettiva perché, se $a \neq 0$, guardando la a-esima componente di $u(a)$,

$$\pi_a u(a) = \vartheta_a(a) = \varphi_a(a) \neq 0 \qquad \square$$

Lo $\mathbb{Z}$-modulo $\prod \mathbb{Q}/\mathbb{Z}$ si dice *colibero*, perché abbiamo appena mostrato che verifica la proprietà duale a quella dei moduli liberi. Dunque nel caso $\Lambda = \mathbb{Z}$ siamo abbastanza soddisfatti. Per "riciclare" questa dimostrazione per Λ generico l'idea è

- Trovare un Λ-modulo che faccia le veci di $\mathbb{Q}/\mathbb{Z}$.
- Dichiarare[23] che un Λ-modulo colibero è un prodotto di copie del Λ-modulo di cui sopra.

Sia Λ un anello. Siano poi A un Λ-modulo *destro*, G uno $\mathbb{Z}$-modulo, e consideriamo $\mathrm{Hom}_{\mathbb{Z}}(A, G)$. Muniamolo di una struttura di Λ-modulo *sinistro* come segue: se $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A, G)$ definiamo $\lambda\varphi(a) = \varphi(a\lambda)$. Insospettiti dall'Osservazione 6.2 andiamo a verificare che il prodotto per scalare è associativo[24], cioè che $(\lambda_1\lambda_2)\varphi = \lambda_1(\lambda_2\varphi)$.

$$((\lambda_1\lambda_2)\varphi)(a) = \underline{\varphi(a(\lambda_1\lambda_2)) = \varphi((a\lambda_1)\lambda_2)} = \lambda_2\varphi(a\lambda_1) = (\lambda_1(\lambda_2\varphi))(a)$$

Occhio alla parte sottolineata: quello che fa funzionare tutto è la scelta furba dell'accoppiata modulo destro/modulo sinistro in corsivo, che permette a λ_2 di agire per primo. La costruzione fatta va bene in particolare quando come Λ-modulo destro prendiamo Λ, è questo è il "surrogato" di $\mathbb{Q}/\mathbb{Z}$ che cercavamo:

Definizione 6.29. Un Λ-modulo sinistro si dice colibero se è isomorfo a $\prod_{i\in I} (\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z}))_i$.

[23] Qui sembra quasi che stiamo bluffando, ma la definizione di "oggetto libero" può essere data anche solo in termini di frecce (cioè in termini categoriali, come vedremo fra poco), e in quel caso è ovvio cosa vuol dire "colibero". Noi rimarremo legati a definizioni più concrete, ma per il lettore che ha apprezzato la nota 18: se invece del funtore dimenticante in Set prendiamo quello in Ab abbiamo a disposizione sia un aggiunto sinistro, che per la cronaca è $\Lambda \otimes_{\mathbb{Z}} -$, che un aggiunto destro, cioè $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, -)$, in cui guarda caso stiamo giusto per imbatterci. Si veda [11]. Comunque durante il corso l'espressione "funtore aggiunto" non è mai stata utilizzata, ma se uno guarda bene l'enunciato del Teorema 6.30...

[24] Ad essere onesti bisognerebbe farsi tutto il resto delle verifiche, ma la parte delicata è questa.

Per vedere che effettivamente funziona passiamo da questa cosa:

Teorema 6.30. Siano A un Λ-modulo sinistro, G un gruppo abeliano e consideriamo $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)$ come Λ-modulo sinistro. Allora esiste un isomorfismo di gruppi abeliani

$$\eta_A \colon \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)) \to \mathrm{Hom}_{\mathbb{Z}}(A, G)$$

Inoltre se $\sigma \colon A \to B$ è un omomorfismo di Λ-moduli sinistri,

$$\begin{array}{ccc} \mathrm{Hom}_{\Lambda}(B, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)) & \xrightarrow{\eta_B} & \mathrm{Hom}_{\mathbb{Z}}(B, G) \\ \Big\downarrow{\scriptstyle \sigma^*} & \circlearrowleft & \Big\downarrow{\scriptstyle \sigma^*} \\ \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)) & \xrightarrow[\eta_A]{} & \mathrm{Hom}_{\mathbb{Z}}(A, G) \end{array}$$

Dimostrazione. Definiamo esplicitamente una mappa che associ ad un omomorfismo $\varphi \in \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G))$ un omomorfismo $\eta_A(\varphi) \in \mathrm{Hom}_{\mathbb{Z}}(A, G)$. Poniamo

$$\eta_A(\varphi)(a) = \varphi(a)(1)$$

e poi c'è da fare tutte le verifiche del mondo[25]. Per facilitarle diciamo che l'inversa è $\eta_A^{-1} = \xi_A \colon \mathrm{Hom}_{\mathbb{Z}}(A, G) \to \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G))$, definita come

$$\xi_A(\psi)(a)(\lambda) = \psi(\lambda a) \qquad a \in A,\ \lambda \in \Lambda$$ □

Teorema 6.31. Ogni Λ-modulo sinistro A può essere immerso in un Λ-modulo colibero.

Dimostrazione. A è anche un gruppo abeliano, per cui come già visto nella dimostrazione del Teorema 6.28 per ogni $a \in A$ diverso da 0 esiste un omomorfismo *di gruppi abeliani* $\vartheta_a \colon A \to \mathbb{Q}/\mathbb{Z}$ tale che $\vartheta_a(a) \neq 0$. Poniamo

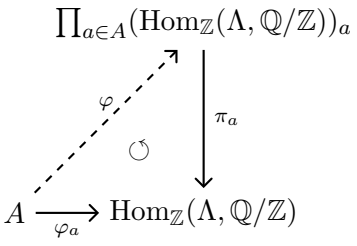
$$\varphi_a = \xi_A(\vartheta_a) \colon A \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$$

Dove ξ_A è la mappa η_A^{-1} definita nella dimostrazione del Teorema precedente. Se $a \neq 0$ abbiamo

$$\varphi_a(a)(1) = \xi_A(\vartheta_a)(a)(1) = \vartheta_a(1 \cdot a) = \vartheta_a(a) \neq 0$$

Dunque, analogamente a quanto fatto nel Teorema 6.28, abbiamo per ogni a una mappa $\varphi_a \colon A \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$ tale che $\varphi_a(a) \neq 0$. Passiamo al prodotto diretto al variare di $a \in A$ ottenendo φ che fa commutare tutti i

[25] Il lettore pigro può consultare [4] a pagina 23.

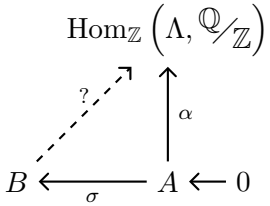


e, sempre come nella dimostrazione del Teorema 6.28, φ è iniettiva perché se $a \neq 0$ allora guardando la a-esima componente di $\varphi(a)$ abbiamo $\pi_a(\varphi(a)) = \varphi_a(a) \neq 0$. □

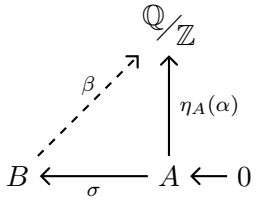
La collana di risultati duali continua con

Teorema 6.32. Ogni Λ-modulo colibero è iniettivo.

Dimostrazione. Dato che il prodotto di moduli iniettivi è iniettivo, basta dimostrare l'iniettività di $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$.



Applicando la η_A del Teorema 6.30 possiamo rimpiazzare $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$ con $\mathbb{Q}/\mathbb{Z}$ e sfruttare l'iniettività di quest'ultimo:



Per ottenere la tesi basta allora "tornare indietro" mettendo $\eta_B^{-1}(\beta)$ al posto del punto interrogativo nel primo diagramma: infatti, ripercorrendosi i diagrammi coinvolti[26], abbiamo

$$\eta_B^{-1}(\beta) \circ \sigma = \sigma^* \circ \eta_B^{-1}(\beta) = \eta_A^{-1} \circ \sigma^*(\beta) = \eta_A^{-1}(\beta \circ \sigma) = \eta_A^{-1}(\eta_A(\alpha)) = \alpha \ \square$$

Dai gli ultimi due risultati dimostrati segue immediatamente che

Corollario 6.33. Ogni Λ-modulo è sottomodulo di un modulo iniettivo.

[26] Cioè questi due e quello del Teorema 6.30. Non c'è bisogno di ridisegnarli: la notazione è "retrocompatibile". Occhio però che stiamo lavorando con le η^{-1}, non con le η.

Teorema 6.34 (di Caratterizzazione dei Moduli Iniettivi)**.** Sono equivalenti:

1. I è iniettivo.
2. Per ogni successione esatta $0 \to A \to B \to C \to 0$ la successione
$$0 \to \mathrm{Hom}(C, I) \to \mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I) \to 0$$
è esatta.
3. Se $0 \to I \xrightarrow{\mu} B$ è esatta allora μ ha un'inversa sinistra.
4. I è addendo diretto di ogni modulo che lo contiene.
5. I è addendo diretto di un modulo colibero.

Strategia di Dimostrazione. Si dualizza l'analogo per i moduli proiettivi utilizzando quanto visto finora[27]. □

6.3 Moduli Piatti su PID

Proposizione 6.35. Se Λ è un PID e M è un Λ-modulo, questo è piatto se e solo se è libero da torsione.

Dimostrazione. Mostriamo prima il "⇒". Dire che M ha un elemento di torsione vuol dire che esistono $a \in \Lambda$ e $m \in M$ non nulli e tali che $am = 0$. Consideriamo
$$0 \to \Lambda \xrightarrow{\cdot a} \Lambda \to {}^{\Lambda}\!/_{\langle a \rangle} \to 0$$
che è esatta perché Λ è un dominio[28]. Guardiamo la successione
$$0 \to \Lambda \otimes M \xrightarrow{\cdot a \otimes \mathrm{id}} \Lambda \otimes M$$
Questa non è esatta perché abbiamo
$$1 \otimes m \xrightarrow{(\cdot a) \otimes \mathrm{id}} a \otimes m = 1 \otimes am = 0$$
Dunque M non è piatto.

Occupiamoci ora del "⇐". Sia M libero da torsione e prendiamo una successione esatta
$$0 \to A' \xrightarrow{\varphi} A \to A'' \to 0$$
per poi tensorizzarla per M
$$0 \to A' \otimes M \xrightarrow{\varphi \otimes \mathrm{id}} A \otimes M \to A'' \otimes M \to 0$$

[27] I dettagli possono essere reperiti in [4], dove questo risultato si chiama Teorema 25 e si trova... a pagina 25.

[28] Effettivamente questa freccia funziona anche se λ è un dominio ma non un PID.

Come noto la questione si risolve nel capire se $\varphi \otimes \mathrm{id}$ è iniettiva. Se non lo fosse ci sarebbero certi, finiti, a_i' ed m_i tali che

$$\Big(\underbrace{\sum a_i' \otimes m_i}_{\neq 0} \Big) \xrightarrow{\varphi \otimes \mathrm{id}} 0$$

il che significa che, in $A \otimes M$, vale

$$\sum \varphi(a_i') \otimes m_i = 0 \tag{6.1}$$

Ricordiamoci la costruzione di $A \otimes M$ come

$$\frac{\text{libero sugli } a \otimes m}{\text{relazioni}}$$

Leggendo la (6.1) nel libero sugli $a \otimes m$ abbiamo

$$\sum \varphi(a_i') \otimes m_i = \text{relazioni (finite)}$$

Dato che queste relazioni sono finite possiamo scegliere un po' di moduli finitamente generati $A_0 \subset A$, $A_0' \subset A'$, $M_0 \subset M$ che contengano quanto serve, cioè tali che $\langle a_i' \rangle \subset A_0'$, $\langle \varphi(a_i') \rangle \subset A_0$, $\langle m_i \rangle \subset M_0$ e tutto quello che serve a scrivere le finite relazioni di cui sopra e ricondurci alla situazione

$$0 \to A_0' \to A_0 \to {}^{A_0}\!/_{\varphi(A_0')} \to 0$$

in cui i moduli sono tutti finitamente generati. Tensorizziamo

$$0 \to A_0' \otimes M_0 \xrightarrow{\varphi \otimes \mathrm{id}} A_0 \otimes M_0$$

e anche qui abbiamo $0 \neq \sum a_i' \otimes m_i \mapsto 0$. Ora però mostriamo (prossima Proposizione) che, se Λ è un PID, ogni Λ-modulo finitamente generato e libero da torsione è libero (e in particolare piatto), e abbiamo ottenuto un assurdo. □

Questa strategia si ricicla: quando lavora con tensori e mappe (non) iniettive ci si riconduce a moduli finitamente generati[29].

Proposizione 6.36. Se Λ è un PID, ogni Λ-modulo finitamente generato e libero da torsione è libero.

Dimostrazione. Siano M il modulo in questione, $\{y_1, \dots, y_m\}$ suoi generatori e $\{v_1, \dots, v_n\}$ un loro sottoinsieme massimale linearmente indipendente[30].

[29] Vedi Corollario 2.13 in [2].

[30] Il fatto che M sia libero da torsione ci dice che, ad esempio, $\{y_1\}$ è linearmente indipendente, per cui $\{v_1, \dots, v_n\} \neq \emptyset$.

Supponiamo che $y_1 \notin \{v_1, \ldots, v_n\}$. Allora per massimalità otteniamo una relazione del tipo

$$\underbrace{a_1}_{\neq 0} y_1 + b_{1,1}v_1 + \ldots + b_{1,n}v_n = 0$$

Chiaramente una cosa del genere la possiamo a maggior ragione scrivere anche se $y_1 \in \{v_1, \ldots, v_n\}$. Lo stesso discorso vale per tutti gli altri y_i, per cui otteniamo delle relazioni

$$\underbrace{a_i}_{\neq 0} y_i + b_{i,1}v_1 + \ldots + b_{i,n}v_n = 0$$

Poniamo $a = \prod a_i$ e notiamo che la mappa $M \xrightarrow{\cdot a} M$ è iniettiva perché M è libero da torsione. Dunque abbiamo, per scelta di a,

$$M \cong aM \subset \langle v_1, \ldots, v_n \rangle \cong \Lambda^n$$

Ma allora M è sottomodulo di un modulo libero finitamente generato, e quindi[31] è libero perché Λ è un PID. □

Un immediato corollario della Proposizione 6.35 è che, ad esempio, $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo piatto.

6.4 Categorie

Definizione 6.37. Una categoria $\mathcal{C}$ è data da

1. Una classe di *oggetti*
2. Per ogni coppia di oggetti A, B, un insieme[32] di *morfismi*[33] $\mathcal{C}(A, B)$

[31] Questo dovrebbe essere un risultato noto da Algebra 2. Comunque una dimostrazione è reperibile in [1], Capitolo VI, Proposizione 5.1.

[32] Per il lettore attento alle questioni set-teoretiche/fondazionali: alcuni autori permettono anche ai morfismi fra due oggetti di essere una classe propria, e chiamano una categoria come l'abbiamo definita noi, cioè dove i morfismi fra due oggetti sono sempre un insieme, *locally small*. Se anche gli oggetti sono un insieme la categoria si dice *small* (piccola). Comunque la nostra trattazione può essere portata avanti senza bluffare all'interno della teoria degli insiemi di Bernays-Gödel. Se non sapete cos'è, diciamo che è un'estensione "safe" (la parola giusta è *conservativa*) di ZFC che permette di parlare di classi a pieno titolo, senza dover ricorrere a metateoremi del tipo "per ogni formula...". Il "safe" vuol dire che ogni risultato che "parla solo di insiemi" e viene dimostrato in Bernays-Gödel, anche utilizzando la cosiddetta "scelta globale" (essenzialmente scelta su classi proprie), può essere dimostrato anche nell'ordinaria ZFC. Ora, questi sono gli appunti di un corso di algebra e quindi ci fermiamo qui, ma se volete sapere come si fa e conoscete un po' di forcing consultate la pagina 237 di [7].

[33] A volte chiamati anche *frecce* o *mappe*. Non sono necessariamente funzioni: possono anche essere relazioni d'ordine parziale o altro, come vedremo fra poco.

3. Per ogni terna di oggetti $A, B, C \in \mathcal{C}$ una funzione detta *legge di composizione* $\circ_{\mathcal{C}} \colon \mathcal{C}(A,B) \times \mathcal{C}(B,C) \to \mathcal{C}(A,C)$

che verificano i seguenti assiomi:

1. Se $A_1 \neq A_2$ o $B_1 \neq B_2$ allora $\mathcal{C}(A_1,B_1) \cap \mathcal{C}(A_2,B_2) = \emptyset$.
2. La composizione di morfismi è associativa.
3. Per ogni $A \in \mathcal{C}$ esiste un morfismo $1_A \in \mathcal{C}(A,A)$ tale che per ogni f e g vale $1_A \circ_{\mathcal{C}} g = g$ e $f \circ_{\mathcal{C}} 1_A = f$.

Definizione 6.38. Siano $\mathcal{D}$ e $\mathcal{C}$ categorie. Diciamo che $\mathcal{D}$ è una *sottocategoria* di $\mathcal{C}$ se

1. Gli oggetti di $\mathcal{D}$ sono una sottoclasse degli oggetti di $\mathcal{C}$
2. Le frecce di $\mathcal{D}$ sono anche in $\mathcal{C}$, cioè $\forall X, Y\ \mathcal{D}(X,Y) \subseteq \mathcal{C}(X,Y)$
3. Non importa dove facciamo le composizioni, cioè se $f \in \mathcal{D}(X,Y)$ e $g \in \mathcal{D}(Y,Z)$, allora $g \circ_{\mathcal{D}} f = g \circ_{\mathcal{C}} f$.

Esempio 6.39. La categoria Set degli insiemi, dove le frecce sono le funzioni. Le categorie $\mathscr{M}_\Lambda^\ell$ e $\mathscr{M}_\Lambda^r$ dei Λ-moduli rispettivamente sinistri e destri[34], dove le frecce sono le applicazioni lineari (omomorfismi di moduli). La categoria Ab dei gruppi abeliani, dove le frecce sono gli omomorfismi di gruppi abeliani.

Esempio 6.40. Un esempio di categoria in cui i morfismi non sono funzioni è fornito da un qualunque insieme parzialmente ordinato $(P, \leq)$, a cui associamo la categoria $\mathcal{P}$ che ha come oggetti gli $x \in P$ e come morfismi le relazioni d'ordine, nel senso che $\mathcal{P}(x,y) \neq \emptyset \Leftrightarrow x \leq y$, e in tal caso contiene solo l'elemento "$x \leq y$".

Le mappe fra categorie si chiamano *funtori*:

Definizione 6.41. Se $\mathcal{C}$, $\mathcal{D}$ sono categorie, un *funtore* $F \colon \mathcal{C} \to \mathcal{D}$ associa ad ogni oggetto $X \in \mathcal{C}$ un oggetto $F(X) \in \mathcal{D}$ e ad ogni $f \in \mathcal{C}(X,Y)$ un morfismo $F(f) \in \mathcal{D}(F(X), F(Y))$ in modo che

1. $F(f \circ_{\mathcal{C}} g) = F(f) \circ_{\mathcal{D}} F(g)$
2. $F(1_X) = 1_{F(X)}$

Esempio 6.42. Il funtore $\pi_1 \colon$ sp. Top. puntati $\to$ Grp, la categoria dei gruppi. Il funtore $F_A \colon \mathscr{M}_\Lambda^\ell \to$ Ab che associa $B \mapsto \mathrm{Hom}_\Lambda(A,B)$, noto anche come $\mathrm{Hom}_\Lambda(A,-)$.

[34] Alcuni autori le indicano rispettivamente con Λ-Mod e Mod-Λ.

Definizione 6.43. Data una categoria $\mathcal{C}$ la sua categoria *opposta* $\mathcal{C}^{\mathrm{op}}$ ha gli stessi oggetti di $\mathcal{C}$ ma le frecce "al contrario", cioè $\mathcal{C}^{\mathrm{op}}(X,Y) = \mathcal{C}(Y,X)$, con la legge di composizione indotta[35] da quella di $\mathcal{C}$.

Definizione 6.44. Un *funtore covariante* è un funtore come l'abbiamo definito prima. Un *funtore controvariante* $\mathcal{C} \to \mathcal{D}$ è un funtore covariante $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

In altre parole è un funtore come l'abbiamo definito prima, salvo che gira le frecce, nel senso che se $f \in \mathcal{C}(X,Y)$ allora $F(f) \in \mathcal{D}(F(Y),F(X))$ e $F(f \circ_{\mathcal{C}} g) = F(g) \circ_{\mathcal{D}} F(f)$.

Esempio 6.45. Un funtore controvariante è $\bar{F}_B \colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ che associa $C \mapsto \mathrm{Hom}_\Lambda(C,B)$, noto anche come $\mathrm{Hom}_\Lambda(-,B)$.

Dato che esiste il funtore identico, uno potrebbe identificare due categorie nella solita maniera, cioè dicendo che un funtore F è un isomorfismo se esiste un funtore G tale che le composizioni $F \circ G$ e $G \circ F$ siano i funtori identici, e che due categorie sono isomorfe se esiste un isomorfismo fra di loro. Contrariamente a quanto ci si possa aspettare, quando si parla di categorie questa *non* è la nozione giusta con cui lavorare, perché è troppo rigida. L'idea di fondo è che, dato che — ad esempio in algebra commutativa — si lavora sempre a meno di isomorfismo, in una categoria uno vorrebbe non distinguere oggetti isomorfi. Quindi se $F \circ G$ non è il funtore identico, ma comunque $F \circ G(X)$ è sempre isomorfo a X *e l'isomorfismo è sufficientemente "bello"*[36] dovremmo essere contenti lo stesso[37]. Dato che le mappe sono parte integrante della loro categoria[38], quel "bello" sta a significare che gli isomorfismi devono rispettare le mappe, ossia essere fatti coerentemente lungo tutta la categoria, nel seguente senso:

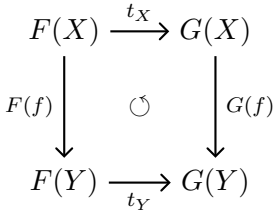
Definizione 6.46. Siano F e G due funtori $\mathcal{C} \to \mathcal{D}$. Una *trasformazione naturale* t tra F e G assegna ad ogni oggetto $X \in \mathcal{C}$ un morfismo $t_X \in \mathcal{D}(F(X),G(X))$ tale che per ogni $f \in \mathcal{C}(X,Y)$

[35] Che, visto che abbiamo girato le frecce, funziona "a rovescio": $(f \circ_{\mathcal{C}} g)^{\mathrm{op}} = g^{\mathrm{op}} \circ_{\mathcal{C}^{\mathrm{op}}} f^{\mathrm{op}}$.

[36] ... e le stesse cose succedono anche per $G \circ F$...

[37] Ad esempio una categoria con due oggetti (con le rispettive identità) e nessuna freccia fra di loro è sostanzialmente diversa da una categoria con due oggetti (e le rispettive identità) e una freccia fra di loro. Se aggiungiamo anche un'inversa per quest'ultima freccia però la categoria si ritrova due oggetti isomorfi e inizia a somigliare molto alla categoria con un solo oggetto e come unica freccia l'identità...

[38] C'è anche una definizione di categoria solo con le frecce, senza oggetti, con l'idea che un oggetto può essere "rimpiazzato" dal suo morfismo identità. Si veda [15].



Inoltre se ogni t_X è un isomorfismo[39] si dice che t è un'*equivalenza naturale*.

La nozione di "categorie isomorfe" è quindi "snobbata" in favore di quella di *categorie equivalenti*:

Definizione 6.47. Un'*equivalenza di categorie* è una coppia di funtori le cui composizioni siano naturalmente equivalenti alle rispettive identità.

Abbiamo già visto un'equivalenza naturale: si confronti l'ultimo diagramma con quello del Teorema 6.30, che però è un'equivalenza naturale fra funtori controvarianti[40]. Ovviamente avere una trasformazione tra F e G non significa averne una tra G e F, esattamente come nel caso delle frecce in una categoria[41]. Per le equivalenze naturali però sì, come si vede facilmente sostituendo tutti i t_X con t_X^{-1}. Può essere utile fare un non-esempio di equivalenza naturale, ossia vedere due funtori che *non* sono naturalmente equivalenti, anche se a prima vista sembrano contenere essenzialmente le stesse informazioni. Si veda l'Esercizio A.15. L'esempio classico di trasformazione naturale (anzi, quello che pare aver motivato la definizione) è il seguente:

Esempio 6.48 (Biduale)**.** Ve la ricordate al primo anno quella storia che uno spazio e il suo duale erano isomorfi, ma uno spazio e il suo biduale erano *più isomorfi*? Che l'isomorfismo era *naturale*?

Consideriamo la categoria $\mathcal{V}_K$ degli spazi vettoriali su K (i morfismi sono le applicazioni lineari) e definiamo la classe di mappe (che sta per diventare una trasformazione naturale) $i = \{i_V \mid V \in \mathcal{V}_K\}$, dove

$$i_V \colon V \to V^{**} \qquad \forall \varphi \in V^* \; i_V(w)(\varphi) = \varphi(w)$$

Consideriamo il funtore identico $\mathrm{Id} \colon \mathcal{V}_K \to \mathcal{V}_K$ e il funtore "duale" $* \colon \mathcal{V}_K \to \mathcal{V}_K$ che associa a V il suo duale V^* e a $\varphi \colon V \to W$ la sua trasposta $\varphi^* \colon W^* \to V^*$, definita da $\varphi^*(f) = f \circ \varphi$. Se ora consideriamo il funtore "biduale" $**$, la i definita sopra è una trasformazione naturale da Id a $**$, e se ci restringiamo agli spazi di dimensione finita[42] $\mathcal{V}_K^{<+\infty}$ è un'equivalenza naturale.

[39] Come ci si aspetta vuol dire che t_X ha un'inversa simultaneamente destra e sinistra; dire "inversa" ha senso perché i morfismi identità esistono sempre.

[40] E che potremmo battezzare $\mathrm{Hom}_\Lambda(-, \mathrm{Hom}_\mathbb{Z}(\Lambda, G))$ e $\mathrm{Hom}_\mathbb{Z}(-, G)$.

[41] Ad esempio in Set, per qualunque insieme X c'è sempre una (sola) funzione $\emptyset \to X$: quella vuota; se $X \neq \emptyset$, però, non esistono funzioni $X \to \emptyset$. Alternativamente, in una categoria/poset, se $x \lneq y$, c'è una freccia $x \to y$ ma nessuna $y \to x$.

[42] Altrimenti i_V non è più detto che sia surgettiva.

$$\begin{array}{ccc} \mathrm{Id}(V) & \xrightarrow{i_V} & V^{**} \\ {\scriptstyle \mathrm{Id}(f)}\downarrow & \circlearrowleft & \downarrow{\scriptstyle f^{**}} \\ \mathrm{Id}(W) & \xrightarrow[i_W]{} & W^{**} \end{array}$$

Anche in dimensione finita comunque i funtori identico e duale *non* sono naturalmente equivalenti. Tanto per cominciare uno è covariante e l'altro controvariante, per cui la definizione di equivalenza naturale come l'abbiamo data noi non ha senso[43]. È anche vero che nessuno ci vieta[44] di provare a dare la stessa definizione ma con una freccia al contrario: possiamo benissimo chiedere che esista una classe di isomorfismi $t = \{t_V \mid V \in \mathcal{V}_K^{<+\infty}\}$ che faccia commutare tutti i diagrammi della forma

$$\begin{array}{ccc} \mathrm{Id}(V) & \xrightarrow{t_V} & V^{*} \\ {\scriptstyle \mathrm{Id}(f)}\downarrow & & \uparrow{\scriptstyle f^{*}} \\ \mathrm{Id}(W) & \xrightarrow[t_W]{} & W^{*} \end{array}$$

Il problema è che per qualunque candidata "equivalenza naturale" t è facile esibire un quadrato come sopra che *non* commuta: del resto andare da V a V^* seguendo il percorso "superiore" non tiene in nessun conto f, mentre seguire il percorso "inferiore" sì, per cui dovremmo già iniziare a sentire puzza di bruciato... Effettivamente basta prendere come V un qualunque spazio vettoriale non nullo, W uno spazio vettoriale qualunque, e come f la mappa nulla. In tal caso l'iniettività di t_V, che stiamo supponendo essere un isomorfismo, non va molto d'accordo con la commutatività del diagramma:

$$t_V = f^* \circ t_W \circ f = f^* \circ t_W \circ 0 = 0$$

Incidentalmente, questo mostra che una qualunque "trasformazione naturale" dal funtore identico a quello duale è quella che manda tutto in 0.

[43] Però, come abbiamo già visto, fra due funtori controvarianti ha senso: semplicemente sono due funtori $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$. Però fra un funtore $\mathcal{C} \to \mathcal{D}$ e uno $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$...

[44] Vedi [9].

Capitolo 7

Funtori Derivati

Vogliamo lavorare con *complessi*, dove un complesso è fatto così

$$\cdots \xrightarrow{\delta_5} P_4 \xrightarrow{\delta_4} P_3 \xrightarrow{\delta_3} P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} 0$$

dove l'immagine di ogni mappa è inclusa nel Ker di quella dopo. Supponiamo che la successione sia esatta. Se ci applichiamo un funtore T troviamo un altro complesso

$$\cdots \xrightarrow{T\delta_5} TP_4 \xrightarrow{T\delta_4} TP_3 \xrightarrow{T\delta_3} TP_2 \xrightarrow{T\delta_2} TP_1 \xrightarrow{T\delta_1} TP_0 \xrightarrow{\delta_0} 0$$

che non è più detto che sia esatto. Uno poi può definire l'omologia misurando "quanto non è esatto" un complesso, tipo ponendo $H_2 = \operatorname{Ker} T\delta_2 / \operatorname{Im} T\delta_3$. Supponiamo ora che il complesso dei P non sia esatto ma lo sia se ci aggiungiamo A:

$$\cdots \to P_4 \to P_3 \to P_2 \to P_1 \to P_0 \to A \to 0$$

applicando T e calcolando l'H_2 salta fuori che la dipendenza è *funtoriale* rispetto ad A, cioè la mappa che associa A ad H_2 dà vita a un funtore. Magari a qualcuno piace di più l'H_4, e possiamo definire un nuovo funtore che manda A in H_4. Questi si chiamano *funtori derivati* associati a T. Questo era un progetto, ora vedremo tutto per bene. Avremo in mente i (bi[1])funtori $\operatorname{Hom}(-,-)$ e $- \otimes -$, i cui funtori derivati sono rispettivamente gli Ext^n e Tor_n cui si accennava qualche pagina fa. Pronti? Via.

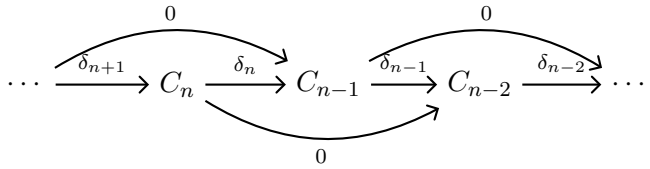
[1]Non stiamo a dare la definizione di bifuntore, ma dovremmo esserci capiti.

7.1 Preliminari

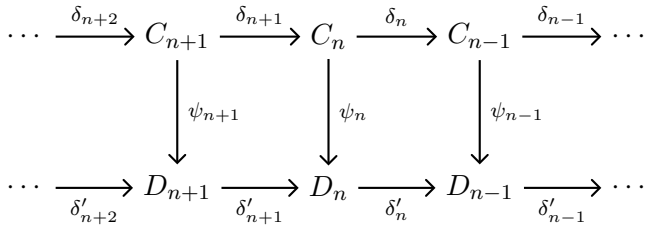
Definiamo la categoria $\mathscr{M}_\Lambda^{\mathbb{Z}}$ nella seguente maniera: gli oggetti sono i Λ-moduli graduati, dove la gradazione è intesa in $\mathbb{Z}$, e non in $\mathbb{N}$ come nella parte di algebra commutativa. In altre parole ora possono esistere anche elementi di grado negativo[2], cioè $A = \oplus_{n\in\mathbb{Z}} A_n$. In questo contesto pensiamo Λ come anello graduato in cui tutti gli elementi hanno grado 0, quindi la moltiplicazione per scalare è un endomorfismo di ogni A_n. I morfismi sono divisi per grado: un *morfismo di grado k* da A a B è una mappa del tipo $\varphi = \{\varphi_i\}$ dove $\varphi_i \colon A_i \to B_{i+k}$. In altre parole è un omomorfismo che manda omogenei di grado i in omogenei di grado $i + k$.

Definizione 7.1. Un *complesso di catene* è dato da un Λ-modulo graduato $C = \{C_n\}$ e un morfismo $\delta = \{\delta_n\} \in \mathscr{M}_\Lambda^{\mathbb{Z}}(C, C)$ di grado -1 tale che $\delta \circ \delta = 0$.

Dunque la situazione è del tipo



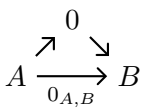
Definizione 7.2. Un *morfismo* fra complessi è una $\psi = \{\psi_n\} \in \mathscr{M}_\Lambda^{\mathbb{Z}}(C, D)$ di grado 0 che fa commutare i[tutti i quadrati de]l diagramma



Possiamo dunque definire la categoria Comp_Λ dei complessi.

Definizione 7.3. Una categoria $\mathcal{U}$ si dice *additiva* se

1. Ha l'oggetto 0, cioè un oggetto tale che per ogni altro oggetto A esiste un unico morfismo $A \to 0$ e un unico morfismo $0 \to A$. In particolare per ogni A, B si può definire un morfismo $0_{A,B}$ come



[2]Questo permette di dare le definizioni in maniera comoda, ma di fatto avremo sempre fra le mani oggetti dove $A_{-n} = (0)$.

2. Ogni coppia di oggetti ha un prodotto[3].
3. Per ogni $A, B \in \mathcal{U}$ i morfismi $\mathcal{U}(A, B)$ formano un gruppo abeliano.
4. La composizione $\mathcal{U}(A, B) \times \mathcal{U}(B, C) \to \mathcal{U}(A, C)$ è bilineare.

Ad esempio $\mathscr{M}_\Lambda^\ell$, $\mathscr{M}_\Lambda^r$, Comp_Λ sono categorie additive.

Definizione 7.4. Un funtore fra categorie additive $T\colon \mathcal{U}_1 \to \mathcal{U}_2$ è *additivo* se per ogni A, B oggetti di $\mathcal{U}_1$ la mappa

$$T\colon \mathcal{U}_1(A, B) \to \mathcal{U}_2(TA, TB)$$

è un omomorfismo di gruppi abeliani.

Per esempio $\mathrm{Hom}(A, -)$, $\mathrm{Hom}(-, A)$, $A \otimes -$, $- \otimes A$ sono additivi.

Osservazione 7.5. Se $T\colon \mathscr{M}_\Lambda^\ell \to \mathscr{M}_{\Lambda'}^\ell$ è additivo e C in Comp_Λ, allora $TC \in \mathrm{Comp}_{\Lambda'}$. In altre parole un funtore additivo manda complessi in complessi[4], per cui T "diventa" anche un funtore $T\colon \mathrm{Comp}_\Lambda \to \mathrm{Comp}_{\Lambda'}$.

Definizione 7.6. Sia $C \in \mathrm{Comp}_\Lambda$ un complesso. Definiamo l'*omologia* $H_*(C) = \{H_n(C)\}$ come il Λ-modulo graduato dato da $H_n(C) = \operatorname{Ker}\delta_n / \operatorname{Im}\delta_{n+1}$. Chiamiamo quest'ultimo *n-esimo modulo[5] di omologia*.

Un morfismo $\psi\colon C \to D$ di complessi induce un morfismo di grado 0 fra le omologie $\psi_*\colon H_*(C) \to H_*(D)$, semplicemente restringendo le ψ_n e passandole al quoziente, cosa possibile per commutatività dei diagrammi nella Definizione 7.2. Infatti

- Quando restringiamo ψ_n a $\operatorname{Ker}\delta_n$ otteniamo una mappa in $\operatorname{Ker}\delta'_n$: infatti se $\delta_n(a) = 0$ allora

$$\delta'_n(\psi_n(a)) = \psi_{n-1}(\delta_n(a)) = \psi_{n-1}(0) = 0$$

- Il passaggio al quoziente ha senso perché se $a = \delta_{n+1}(b)$ allora

$$\psi_n(a) = \psi_n(\delta_{n+1}(b)) = \delta'_{n+1}(\psi_{n+1}(b))$$

  il che significa $a \in \operatorname{Im}\delta_{n+1} \Rightarrow \psi_n(a) \in \operatorname{Im}\delta'_{n+1}$.

In effetti H_* è un funtore: la corrispondenza che abbiamo appena descritto commuta con la composizione e rispetta le identità, e la stessa cosa è vera per tutti gli H_n.

[3] Nel senso della proprietà universale, cioè della Definizione 6.5.

[4] Bisogna preservare $\delta \circ \delta = 0$ e l'additività implica che l'omomorfismo nullo vada nell'omomorfismo nullo.

[5] Se $\Lambda = \mathbb{Z}$ si parla di *gruppi* di omologia.

C'è una definizione analoga per la *coomologia* H^*. Bisogna prendere le cocatene, che sono come le catene ma con le frecce al contrario (dunque $\delta_n \colon C_{n-1} \to C_n$ è un morfismo di grado $+1$), e $H^n = \operatorname{Ker} \delta_{n+1} / \operatorname{Im} \delta_n$.

Attenzione: in [6], [12], e in generale in buona parte della letteratura, la notazione è shiftata di 1: le mappe fra cocatene sono $\delta_n \colon C_n \to C_{n+1}$ e la definizione di coomologia è $H^n = \operatorname{Ker} \delta_n / \operatorname{Im} \delta_{n-1}$ (dunque anche se il nostro δ_n è diverso da quello di [6], gli H^n sono uguali). Tuttavia fra non molto avremo fra le mani scritture del tipo $T\delta_1 \colon TP_0 \to TP_1$ (e non è un caso: viene fuori applicando un funtore controvariante a un complesso di catene, dove si ha $\delta_1 \colon P_1 \to P_0$), per cui per ragioni di sanità mentale ho preferito adottare la notazione attuale[6] piuttosto che dover convivere con un off-by-one perenne in cui la "δ_n" del complesso TP si chiama $T\delta_{n+1}$. Comunque in buona parte della letteratura (ma non in questi appunti) i pedici sotto i δ vengono abbandonati subito dopo aver definito omologia e coomologia, per cui non ci dovrebbero essere (spero) problemi di confusione notazionale nel leggere questi appunti contemporaneamente ai testi suggeriti in bibliografia. Forse la maniera migliore per non confondersi è ricordarsi delle mappe coinvolte nella definizione di H^n come "quella che esce da C_n" e "quella che entra in C_n".

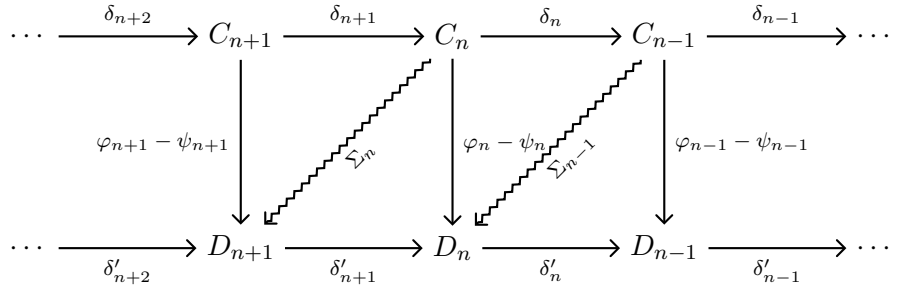
Siano C e D due complessi di catene e $\varphi, \psi \colon C \to D$ due morfismi di complessi. Consideriamo le mappe indotte in omologia $H_*(C) \xrightarrow{\varphi_*} H_*(D)$ e $H_*(C) \xrightarrow{\psi_*} H_*(D)$. Possiamo capire se $\varphi_* = \psi_*$? Una condizione sufficiente perché ciò accada è che fra loro esista un'omotopia, che definiamo subito:

Definizione 7.7. Siano C, D, φ, ψ come sopra. Un'*omotopia* fra φ e ψ è un morfismo $\Sigma \colon C \to D$ di Λ-moduli graduati di grado $+1$ tale che, indicando con δ le mappe di C e con δ' quelle di D,

$$\varphi - \psi = \delta' \circ \Sigma + \Sigma \circ \delta$$

ossia per ogni n vale[7]

$$\psi_n - \varphi_n = \delta'_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \delta_n$$



[6] Che non mi sono inventato io, ad esempio è la stessa usata su Wikipedia.

[7] Il fatto che quelle frecce siano a zigzag indica che per colpa loro il diagramma *non* commuta. Infatti se uno guarda bene la relazione che devono soddisfare...

Come promesso,

Proposizione 7.8. Se φ e ψ sono omotope allora $\varphi_* = \psi_*$.

Dimostrazione. Bisogna vedere che se $[z] \in H_n(C)$, con $z \in \operatorname{Ker} \delta_n$, allora si ha $[(\varphi_n - \psi_n)(z)] = [0] \in H_n(D)$. Ma per definizione di omotopia

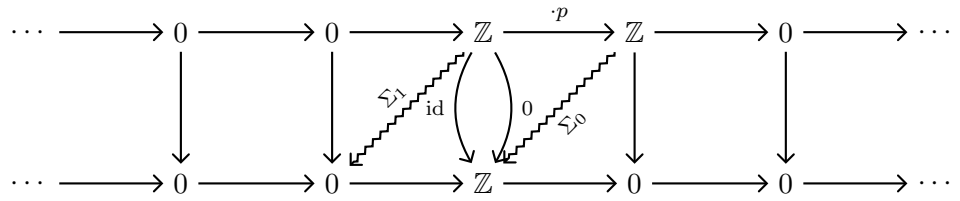
$$(\varphi_n - \psi_n)(z) = \delta'_{n+1} \circ \Sigma_n(z) + \underbrace{\Sigma_{n-1} \circ \delta_n(z)}_{=0}$$

e dunque $(\varphi_n - \psi_n)(z) \in \operatorname{Im} \delta'_{n+1}$. □

Osservazione 7.9. Questo fatto viene utilizzato spesso per mostrare che un complesso ha omologia nulla: basta infatti mostrare che l'identità e la mappa nulla sono omotope, perché in tal caso indurranno in omologia la stessa mappa $\mathrm{id}_* = 0_*$, e non c'è speranza che questo sia vero a meno che gli H_n non siano tutti nulli.

La prossima domanda è: oltre che sufficiente, la condizione è anche necessaria? No: ci sono morfismi non omotopi ma che inducono la stessa mappa in omologia.

Controesempio 7.10. Sia C il complesso della riga superiore, D quello della riga inferiore, $\varphi_1 = \mathrm{id}$, $\psi_1 = 0$, $\psi_n = \varphi_n = 0$ per $n \neq 1$



I primi due gruppi di omologia di questi complessi sono

$$\begin{aligned} H_0(C) &= \mathbb{Z}/p\mathbb{Z} & H_0(D) &= 0 \\ H_1(C) &= 0 & H_1(D) &= \mathbb{Z} \end{aligned}$$

mentre chiaramente gli altri sono tutti nulli. È immediato notare che $\varphi_* = \psi_*$, dato che entrambe non possono che essere la mappa nulla, però se esistesse un'omotopia avremmo l'assurdo

$$1 = (\varphi_1 - \psi_1)(1) = (\delta' \circ \Sigma_1 + \Sigma_0 \circ \delta)(1) = \Sigma_0(p) = p\Sigma_0(1)$$

Proposizione 7.11. Sia $F\colon \mathscr{M}^{\ell}_{\Lambda} \to \mathscr{M}^{\ell}_{\Lambda'}$ un funtore additivo, $C, D \in \mathrm{Comp}_{\Lambda}$ e siano $\varphi, \psi\colon C \to D$ omotope tramite Σ. Allora $F(\varphi)$ è omotopa a $F(\psi)$ e l'omotopia è $F(\Sigma)$.

Dimostrazione. Da $\varphi - \psi = \delta' \circ \Sigma + \Sigma \circ \delta$ abbiamo

$$F(\varphi) - F(\psi) = F(\varphi - \psi) = F(\delta') \circ F(\Sigma) + F(\Sigma) \circ F(\delta)$$

dove la prima uguaglianza vale per additività del funtore F. □

Definizione 7.12. Due complessi hanno lo stesso tipo di omotopia se esistono $\varphi\colon C \to D$ e $\vartheta\colon D \to C$ tali che $\vartheta \circ \varphi$ è omotopa a id_C e $\varphi \circ \vartheta$ è omotopa a id_D.

Osservazione 7.13. Nella situazione sopra, $H_*(C) \cong H_*(D)$, e anzi φ_* e ϑ_* sono isomorfismi.

Definizione 7.14. Sia A un Λ-modulo. Una *risoluzione proiettiva* di A è un complesso P

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\vartheta} P_0 \longrightarrow 0$$

tale che

1. Se $n < 0$ allora $P_n = 0$ (diciamo che P è *positivo*)
2. Ogni P_j è proiettivo
3. $\operatorname{Coker} \vartheta = H_0(P) \cong A$
4. Per ogni $n \geq 1$ vale $H_n(P) = 0$ (diciamo che P è *aciclico*)

In particolare la seguente successione è esatta:

$$\cdots \to P_4 \to P_3 \to P_2 \to P_1 \to P_0 \to A \to 0$$

Spesso e volentieri, quando la situazione non è ambigua, scriveremo cose come "la risoluzione $\cdots \to P_1 \to P_0 \to A \to 0$", intendendo che A non fa parte del complesso P e che la situazione è come quella appena descritta, oppure disegneremo qualcosa del tipo

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_n & \longrightarrow & P_{n-1} & \longrightarrow & \cdots & \longrightarrow & P_1 & \xrightarrow{\vartheta} & P_0 \longrightarrow 0 \\ & & & & & & & & & & \searrow \quad \nearrow \\ & & & & & & & & & & A \end{array}$$

Quali $A \in \mathscr{M}_\Lambda^\ell$ ammettono una risoluzione proiettiva? Tutti. Questo sostanzialmente segue dal fatto che ogni modulo è quoziente di un modulo libero e che i moduli liberi sono proiettivi: si può scrivere A come quoziente di un modulo libero con la proiezione $\pi\colon F_0 \to A$, poi fare lo stesso con $\operatorname{Ker} \pi$ trovando una proiezione $\pi_1\colon F_1 \to \operatorname{Ker} \pi$ per un altro opportuno F_1 libero, e iterare. Questo mostra il risultato più forte che ogni modulo ha

una *risoluzione libera*, la cui definizione è identica a quella di risoluzione proiettiva a parte per la richiesta — più stringente — che ogni F_i sia libero.

C'è anche il concetto duale di *risoluzione iniettiva*, dove le frecce sono tutte al contrario, i Coker diventano Ker e viceversa, il complesso è formato da moduli iniettivi e ad essere nulli sono gli H^n (per $n \geq 1$). Per mostrare che ogni modulo ha una risoluzione iniettiva si dualizza la costruzione precedente, rimpiazzando "ogni modulo è quoziente di un modulo libero" con il Corollario 6.33. Anche questa volta la stessa argomentazione mostra che ogni modulo ha una *risoluzione colibera*, semplicemente usando direttamente il Teorema 6.31 invece del Corollario 6.33.

7.2 Costruzione

Siamo pronti a costruire i funtori derivati. Vedremo nel dettaglio la costruzione dei *funtori derivati sinistri* L_nT di un funtore covariante T. La costruzione dei suoi *funtori derivati destri* R^nT richiede poche modifiche, di cui ci occuperemo a costruzione finita. Si può parlare di L_nT ed R^nT anche nel caso in cui T sia un funtore controvariante, e sempre ad un prezzo (in modifiche alla costruzione) modesto, che pagheremo a fine sezione.

Sia $T\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ un funtore additivo covariante. Il suo *n-esimo funtore derivato sinistro* L_nT è definito come segue. Dati $A \in \mathscr{M}_\Lambda^\ell$ e P una sua risoluzione proiettiva

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0, \qquad P_0 \searrow A \nearrow 0$$

si applica T al complesso dei P

$$\cdots \longrightarrow TP_n \longrightarrow TP_{n-1} \longrightarrow \cdots \longrightarrow TP_1 \longrightarrow TP_0 \longrightarrow 0$$

e se ne calcola l'n-esimo gruppo[8] di omologia $H_n(TP)$. Come il lettore avrà intuito, si pone $L_nT(A) = H_n(TP)$. Dato che a destra compare una P e a sinistra no e che avevamo promesso di definire un *funtore*, e non una mappa qualunque, dobbiamo:

- assicurarci che $L_nT(A)$ non dipenda (modulo isomorfismo) dalla scelta della risoluzione proiettiva P. Finché non l'avremo mostrato, indicheremo $H_n(TP)$ con $L_n^PT(A)$;
- dire cosa fa L_nT sulle mappe.

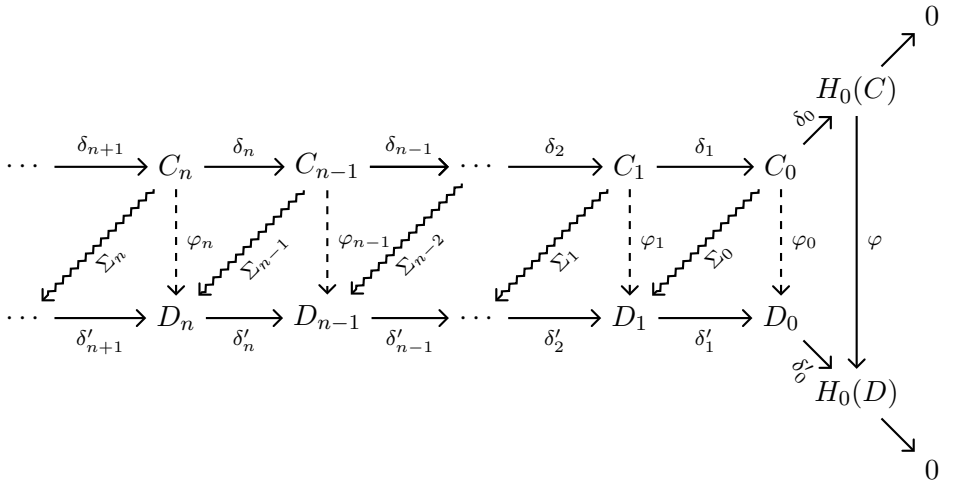
[8]Gruppo, e non modulo: ricordiamo che T restituisce un gruppo abeliano.

Quando diciamo "non dipende dalla scelta della risoluzione proiettiva" stiamo dicendo che se P e Q sono due risoluzioni proiettive di A allora $L_n^P T(A) \cong L_n^Q T(A)$. Dato che per dire cosa fa $L_n T$ sulle mappe useremo comunque le risoluzioni, per non barare bisogna anche mostrare che l'isomorfismo commuta con le mappe, cioè che

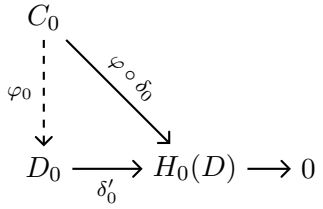
- L'isomorfismo $L_n^P T(A) \cong L_n^Q T(A)$ è naturale.

Tutti e tre i punti precedenti si sistemano più o meno con la stessa idea: si solleva una mappa $A \to A'$ a una mappa fra due loro risoluzioni proiettive, e poi la si passa all'omologia. Il sollevamento non sarà univocamente determinato, nemmeno a risoluzioni fissate, ma la sua classe in omologia sì. Condensiamo tutto il "lavoro sporco" nel seguente

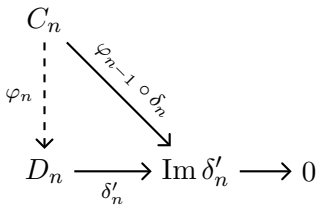
Teorema 7.15. Siano C, D complessi di catene positivi con C proiettivo e D aciclico. Allora per ogni $\varphi\colon H_0(C) \to H_0(D)$ esiste una mappa di complessi $\bar{\varphi} = \{\varphi_n\}$ che solleva φ. Inoltre due tali mappe sono omotope.



Dimostrazione. La dimostrazione è per induzione su n. Il passo base è immediato: φ_0 esiste per proiettività di C_0.



Per il passo induttivo supponiamo di avere $\varphi_0, \ldots, \varphi_{n-1}$, con φ_k che solleva φ_{k-1}. Per commutatività abbiamo $\delta'_{n-1} \circ \varphi_{n-1} \circ \delta_n = \varphi_{n-2} \circ \delta_{n-1} \circ \delta_n = 0$ e usando l'aciclicità di D ne segue $\operatorname{Im}(\varphi_{n-1} \circ \delta_n) \subseteq \operatorname{Ker} \delta'_{n-1} = \operatorname{Im} \delta'_n$. A questo punto possiamo ottenere φ_n invocando la proiettività di C_n sul diagramma



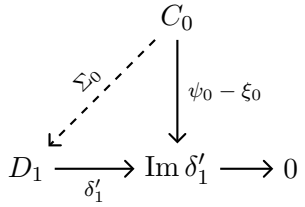
Vediamo, sempre per induzione su n, l'unicità a meno di omotopia. Dati due sollevamenti ψ e ξ vogliamo trovare Σ tale che, per ogni n,

$$\psi_n - \xi_n = \delta'_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \delta_n$$

Definiamo $\Sigma_{-1} \colon H_0(C) \to D_0$ come la mappa nulla. Dato che per ipotesi sia ψ_0 che ξ_0 sollevano φ, allora, per commutatività

$$\delta'_0 \circ (\psi_0 - \xi_0) = (\varphi - \varphi) \circ \delta_0 = 0 \tag{7.1}$$

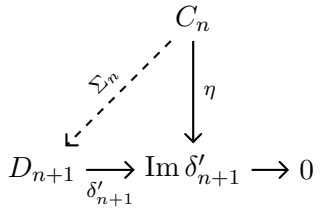
Per commutatività e aciclicità allora $\operatorname{Im}(\psi_0 - \xi_0) \subseteq \operatorname{Ker} \delta'_0 = \operatorname{Im} \delta'_1$, per cui Σ_0 esiste per proiettività di C_0 applicata al diagramma



e abbiamo $\psi_0 - \xi_0 = \delta'_1 \circ \Sigma_0$ che, contando che abbiamo definito $\Sigma_{-1} = 0$, è la tesi. Per il passo induttivo supponiamo di avere costruito le mappe fino alla Σ_{n-1} e costruiamo la Σ_n. Poniamo $\eta = (\psi_n - \xi_n) - (\Sigma_{n-1} \circ \delta_n)$ e abbiamo

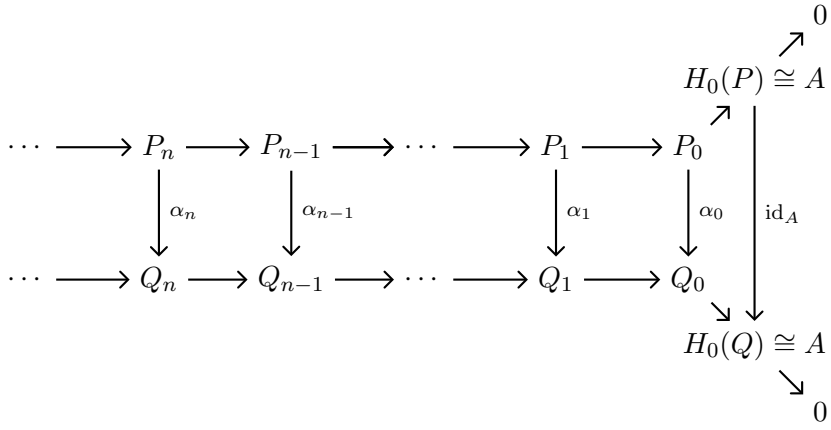
$$\begin{aligned}
&\delta'_n \circ \eta = \delta'_n \circ (\psi_n - \xi_n) - \delta'_n \circ (\Sigma_{n-1} \circ \delta_n) && \text{per additività} \\
&= \delta'_n \circ (\psi_n - \xi_n) - (\delta'_n \circ \Sigma_{n-1}) \circ \delta_n && \text{per associatività} \\
&= (\psi_{n-1} - \xi_{n-1}) \circ \delta_n - (\delta'_n \circ \Sigma_{n-1}) \circ \delta_n && \text{come nella (7.1)} \\
&= (\psi_{n-1} - \xi_{n-1}) \circ \delta_n - (\psi_{n-1} - \xi_{n-1} - \Sigma_{n-2} \circ \delta_{n-1}) \circ \delta_n && \text{induttivamente} \\
&= 0 && \text{perché } \delta \circ \delta = 0
\end{aligned}$$

e dunque $\operatorname{Im} \eta \subseteq \operatorname{Ker} \delta'_n = \operatorname{Im} \delta'_{n+1}$, e Σ_n esiste per proiettività di C_n:



e che questo triangolo commuti vuol dire $\delta'_{n+1} \circ \Sigma_n = \eta$, che scritta per esteso è proprio l'equazione richiesta dall'omotopia. □

Torniamo quindi alla situazione iniziale, con $T\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ covariante additivo, P, Q due risoluzioni proiettive di $A \in \mathscr{M}_\Lambda^\ell$ e verifichiamo che $L_n^P T(A) \cong L_n^Q T(A)$. Usiamo il Teorema precedente per sollevare l'identità[9] $A \to A$ a un morfismo di complessi $\alpha\colon P \to Q$

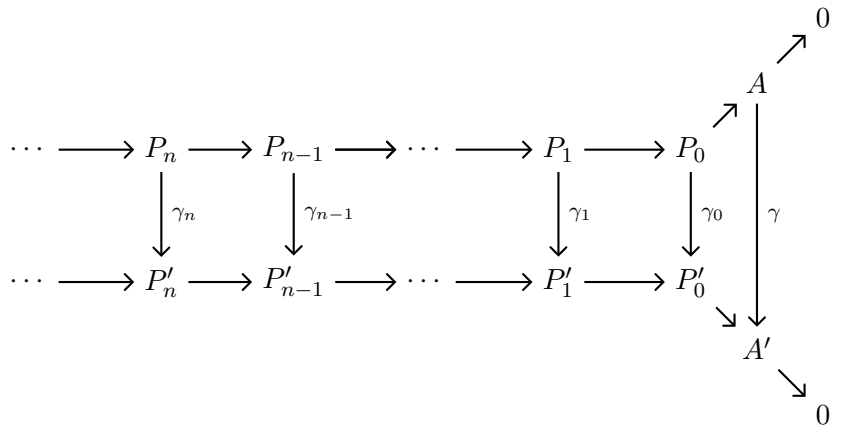


Alla stessa maniera id_A può essere sollevata a un morfismo $\beta\colon Q \to P$ scambiando i ruoli di P e Q nel diagramma sopra. Ma allora $\beta \circ \alpha\colon P \to P$ e $\mathrm{id}\colon P \to P$ sono entrambi sollevamenti dell'identità, dunque sono omotopi, e lo stesso discorso vale per $\alpha \circ \beta\colon Q \to Q$. Dato che mappe omotope inducono le stesse mappe in omologia abbiamo mostrato che $H_*(\beta \circ \alpha)$ e $H_*(\alpha \circ \beta)$ sono le identità di $H_*(P)$ e $H_*(Q)$, per cui $H_*(\alpha)$ e $H_*(\beta)$ sono isomorfismi. Ma allora, dato che T è un funtore additivo, ad esempio, $T(\beta \circ \alpha)$ è ancora omotopa a $T(\mathrm{id})$, per cui ripetendo il ragionamento precedente anche $H_*(T\alpha)\colon H_*(TP) \to H_*(TQ)$ è un isomorfismo, con inversa $H_*(T\beta)$, e non dipende da α perché α è unico a meno di omotopia[10], per cui possiamo battezzarlo $\eta_{P,Q}\colon H_*(TP) \to H_*(TQ)$. In particolare $\eta_{P,Q}$ fornisce gli isomorfismi cercati $\eta_{P,Q,n}\colon H_n(TP) \to H_n(TQ)$, cioè $L_n^P T(A) \to L_n^Q T(A)$.

Occupiamoci ora della parte "mappe" di L_nT. Data $\gamma\colon A \to A'$, scegliamo due risoluzioni proiettive P, P' di A e A' e solleviamo, sempre tramite il Teorema 7.15:

[9] O, ad essere pignoli, la mappa indotta dagli isomorfismi $H_0(P) \cong A \cong H_0(Q)$.

[10] In tutto questo discorso stiamo usando ripetutamente le Proposizioni 7.8 e 7.11 e il Teorema 7.15.



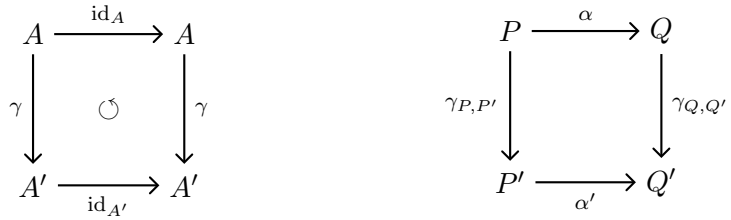
Chiaramente il candidato per $L_nT(\gamma)$ è γ_n passata alle omologie, cioè

$$L_nT(\gamma) = H_n(T\bar{\gamma})\colon L_nT(A) \to L_nT(A')$$

che non dipende dal sollevamento $\bar{\gamma}$ scelto sempre per le Proposizioni 7.8 e 7.11 e il Teorema 7.15; inoltre H_n è un funtore, per cui l'associazione rispetta composizioni e identità. Per non barare però dobbiamo mostrare che anche la parte "mappe" di L_nT non dipende dalle risoluzioni proiettive scelte, ossia se scegliamo altre due risoluzioni Q, Q' gli isomorfismi η definiti prima portano le $L_nT(\gamma)$ definite rispettivamente con P, P' o con Q, Q' nella stessa mappa. In sostanza bisogna mostrare la commutatività di

$$\begin{array}{ccc} L_n^P T(A) & \xrightarrow{\eta_{P,Q,n}} & L_n^Q T(A) \\ \Big\downarrow{\scriptstyle L_n^{P,P'}T(\bar{\gamma})} & & \Big\downarrow{\scriptstyle L_n^{Q,Q'}T(\bar{\gamma})} \\ L_n^{P'} T(A') & \xrightarrow[\eta_{P',Q',n}]{} & L_n^{Q'} T(A') \end{array}$$

Per farlo solleviamo il diagramma di sinistra a quello di destra:



Il quadrato a destra non è detto che commuti, però lo fa a meno di omotopia, perché $\gamma_{Q,Q'} \circ \alpha$ e $\alpha' \circ \gamma_{P,P'}$ sono due sollevamenti $P \to Q'$ di $\gamma\colon A \to A'$ per cui[11] abbiamo la commutatività del primo diagramma (il rettangolo), e quindi la buona definizione degli L_nT.

[11] Usando per l'ennesima volta il Teorema 7.15 e le Proposizioni 7.8 e 7.11.

La costruzione dei *funtori derivati destri* di T è del tutto analoga, ma usando una risoluzione iniettiva. Ad esempio, se T è covariante, per calcolare l'*n-esimo funtore derivato destro* di T, denotato come R^nT, in A si prende una sua risoluzione iniettiva $0 \to A \to I_0 \to I_1 \to \cdots$ e si pone $R^nT(A) = H^n(TI)$. Il duale del Teorema 7.15 è

Teorema 7.16. Siano C, D complessi di cocatene positivi con D iniettivo e C aciclico. Allora ogni $\varphi\colon H^0(C) \to H^0(D)$ si solleva ad un morfismo di complessi $\bar{\varphi}$ unico a meno di omotopia[12].

Se T è controvariante i ruoli si scambiano: per calcolare i suoi funtori derivati sinistri in A si usa una risoluzione iniettiva I e si pone $L_nT(A) = H_n(TI)$, e per i suoi funtori derivati destri si usa una risoluzione proiettiva P e si pone $R^nT(A) = H^n(TP)$.

7.3 Ext e Tor

Definizione 7.17. Ext^n e Tor_n sono gli n-esimi funtori derivati rispettivamente destro di $\mathrm{Hom}_\Lambda(-, B)\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ e sinistro di $A \otimes_\Lambda -\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$, calcolati con le risoluzioni proiettive come nella sezione precedente.

$$\mathrm{Ext}^n_\Lambda(A, B) = R^n \mathrm{Hom}_\Lambda(-, B)(A)$$
$$\mathrm{Tor}^\Lambda_n(A, B) = L_n(A \otimes_\Lambda -)(B)$$

Osservazione 7.18. $\mathrm{Ext}^0(A, B) \cong \mathrm{Hom}(A, B)$ e $\mathrm{Tor}_0(A, B) \cong A \otimes B$.

Dimostrazione. Dato che $T = \mathrm{Hom}(-, B)$ è esatto a sinistra, dall'esattezza di $P_1 \to P_0 \to A \to 0$ segue quella di

$$0 \to TA \to TP_0 \xrightarrow{T\delta_1} TP_1$$

e $H^0(TP) = \mathrm{Ker}\, T\delta_1 \cong TA$. Invece $T = A \otimes -$ è esatto a destra, per cui

$$TP_1 \xrightarrow{T\delta_1} TP_0 \to TB \to 0$$

è esatta e $H_0(TP) = \mathrm{Coker}\, T\delta_1 \cong TB$. Sia in questo caso che in quello precedente è possibile verificare che gli isomorfismi sono naturali, cioè che T e il suo funtore derivato sono naturalmente equivalenti. □

I nomi "Tor" ed "Ext" vengono dal fatto che Tor_1 "estrae" la parte di torsione, mentre vedremo nella prossima sezione che $\mathrm{Ext}^1(A, B)$ "misura" le successioni esatte

$$0 \to B \to E \to A \to 0$$

[12] In questo contesto le omotopie hanno grado -1 invece che $+1$ e la formula da soddisfare è $\varphi_n - \psi_n = \Sigma_n \circ \delta_{n+1} + \delta'_n \circ \Sigma_{n-1}$.

nel senso che è un gruppo abeliano in corrispondenza biunivoca con gli E che contengono B e si quozientano su A (a meno di una certa relazione di equivalenza).

Il fatto che i funtori derivati non dipendano dalla risoluzione proiettiva scelta non solo ne assicura la buona definizione, ma permette di calcolarli usando risoluzioni particolarmente furbe. Ad esempio se B è proiettivo una sua risoluzione proiettiva è

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots \longrightarrow 0 \longrightarrow \underbrace{B}_{=P_0} \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$B$$

Di conseguenza, applicando il tensore abbiamo

$$\cdots \to A \otimes 0 \to A \otimes 0 \to A \otimes B \to 0$$

il che mostra che

Proposizione 7.19. Se B è proiettivo per ogni $n \geq 1$ vale $\mathrm{Tor}_n(A, B) = 0$.

Lo stesso discorso funziona anche per gli Ext^n:

Proposizione 7.20. Se A è proiettivo per ogni $n \geq 1$ vale $\mathrm{Ext}^n(A, B) = 0$.

Un'altra maniera di calcolare i primi ($n = 1$) funtori derivati è usare non le risoluzioni, ma le *presentazioni* proiettive, cosa che faremo spesso, dato che per costruire una presentazione basta cominciare a costruire una risoluzione e fermarsi al primo passo:

Definizione 7.21. Una *presentazione proiettiva* di un Λ-modulo A è una successione esatta corta

$$0 \longrightarrow R \longrightarrow P \longrightarrow A \longrightarrow 0$$

dove P è proiettivo.

Proposizione 7.22 (delle Risoluzioni Proiettive Interrotte)**.** Supponiamo di avere una successione esatta

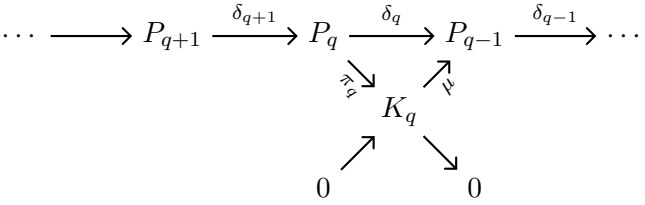
$$0 \to K_q \xrightarrow{\mu} P_{q-1} \to \cdots \to P_1 \to P_0 \to A \to 0$$

dove i P_j sono proiettivi[13]. Sia T un funtore covariante additivo esatto a destra. Allora

$$L_q T(A) \cong \mathrm{Ker}\, T\mu$$

[13]Ma K_q non necessariamente (e chiaramente nemmeno A).

Dimostrazione. "Allunghiamo" la successione risolvendo proiettivamente K_q:



dove $\delta_q = \mu \circ \pi_q$ per definizione . Usando l'esattezza a destra di T sulla "riga storta" che finisce in K_q e "sdoppiando" TP_{q-1} otteniamo il diagramma commutativo

$$\begin{array}{ccccccccc} & & TP_{q+1} & \xrightarrow{T\delta_{q+1}} & TP_q & \xrightarrow{T\pi_q} & TK_q & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle T\delta_q} & & \downarrow{\scriptstyle T\mu} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & TP_{q-1} & \xrightarrow[\mathrm{id}]{} & TP_{q-1} & & \end{array}$$

E per il Lemma del Serpente abbiamo la successione esatta

$$TP_{q+1} \xrightarrow{T\delta_{q+1}} \operatorname{Ker} T\delta_q \to \operatorname{Ker} T\mu \to 0 \to \text{ cose che non ci interessano}$$

che si legge

$$\operatorname{Ker} T\mu \cong \frac{\operatorname{Ker} T\delta_q}{\operatorname{Im} T\delta_{q+1}} = H_q(TP) = L_qT(A) \qquad \square$$

Nel caso di $\operatorname{Tor}_1(A, B)$ dunque, invece della costruzione mediante una risoluzione proiettiva, consideriamo una presentazione proiettiva di B e definiamo $\operatorname{Ker} T\mu = \operatorname{Tor}(A, B)$ e basta, senza l'1 a pedice

$$0 \to K_1 \xrightarrow{\mu} P_0 \to B \to 0$$

Allora $\operatorname{Tor}_1(A, B) = L_1(A \otimes -)(B) \cong \operatorname{Ker}(A \otimes K_1 \to A \otimes P_0) = \operatorname{Tor}(A, B)$. Dunque Tor misura "quanto non è esatta" a sinistra la successione coi tensori. Si può mostrare che anche Tor è un funtore, e che l'isomorfismo è naturale, cioè Tor e Tor_1 sono naturalmente equivalenti (quello che abbiamo fatto noi è solo esibire un isomorfismo fra ogni coppia di oggetti).

Un discorso simile vale per Ext: la Proposizione delle Risoluzioni Proiettive Interrotte ne ha una duale, la cui dimostrazione è analoga:

Proposizione 7.23. Supponiamo di avere una successione esatta

$$0 \to K_q \xrightarrow{\mu} P_{q-1} \to \cdots \to P_1 \to P_0 \to A \to 0$$

con i P_j proiettivi. Sia poi T un funtore controvariante additivo esatto a sinistra[14]. Allora $R^qT(A) \cong \operatorname{Coker} T\mu$.

Dunque, mentre Ext^1 è il primo gruppo di coomologia H^1 del complesso

$$0 \to \operatorname{Hom}(P_0, B) \to \operatorname{Hom}(P_1, B) \to \operatorname{Hom}(P_2, B) \to \cdots$$

possiamo definire $\operatorname{Ext}(A, B)$ (senza l'1 ad apice) passando da una presentazione proiettiva di A

$$0 \to R \xrightarrow{\mu} P \to A \to 0$$

applicando $\operatorname{Hom}(-, B)$ otteniamo

$$0 \to \operatorname{Hom}(A, B) \to \operatorname{Hom}(P, B) \xrightarrow{T\mu} \operatorname{Hom}(R, B)$$

e per la Proposizione precedente

$$\operatorname{Ext}^1(A, B) \cong \operatorname{Coker} T\mu = \operatorname{Hom}(R, B)/\operatorname{Im} T\mu = \operatorname{Ext}(A, B)$$

Anche questa volta salta fuori che Ext^1 ed Ext sono naturalmente equivalenti.

$\operatorname{Ext}^n(A, B)$ può essere calcolato anche risolvendo B, invece che A: prendiamo una risoluzione iniettiva di B

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & I_0 & \longrightarrow & I_1 & \longrightarrow & I_2 & \longrightarrow & I_3 & \longrightarrow & \cdots \\ & \searrow & & \nearrow & & & & & & & \\ & & B & & & & & & & & \end{array}$$

applichiamoci $\operatorname{Hom}(A, -)$ e otteniamo

$$0 \to \operatorname{Hom}(A, B) \to \operatorname{Hom}(A, I_1) \to \operatorname{Hom}(A, I_2) \to \cdots$$

e definiamo $\overline{\operatorname{Ext}}^n(A, -)$ come $R^n \operatorname{Hom}(A, -)$, cioè come l'$n$-esimo funtore derivato destro di $\operatorname{Hom}(A, -)$. Anche se non lo dimostriamo, enunciamo che

Fatto 7.24. $\overline{\operatorname{Ext}}^n$ ed Ext^n sono bifuntori naturalmente equivalenti.

7.4 Estensioni di Moduli

Definizione 7.25. Siano A, B due Λ-moduli sinistri. Un'*estensione di A tramite B* è una successione esatta corta della forma

$$0 \to B \to E \to A \to 0$$

Chiameremo *estensione banale* l'estensione

$$0 \to B \to B \oplus A \to A \to 0$$

[14] Ad esempio $\operatorname{Hom}(-, B)$, che è quello che usiamo per calcolare gli Ext^n con le risoluzioni proiettive.

Chiaramente l'estensione banale c'è sempre. Il funtore Ext parla proprio di queste estensioni, o meglio di queste estensioni modulo la seguente relazione di equivalenza:

Definizione 7.26. Due estensioni di A tramite B si dicono equivalenti se esiste ψ tale che

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 0 & \longrightarrow & B & \longrightarrow & E_2 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Osservazione 7.27. Per la Proposizione 6.9 se una tale ψ esiste è automaticamente un isomorfismo.

Consideriamo il bifuntore

$$E\colon (\mathscr{M}_\Lambda^\ell)^{\mathrm{op}} \times \mathscr{M}_\Lambda^\ell \to \mathrm{Set}$$

che manda (A, B) nell'insieme delle classi di equivalenza delle estensioni di A tramite B. Per come l'abbiamo scritto è evidente che è controvariante nella prima entrata e covariante nella seconda.

Definizione 7.28. Sia Ab la categoria dei gruppi abeliani e sia Set la categoria degli insiemi. Definiamo il funtore $D\colon \mathrm{Ab} \to \mathrm{Set}$, che associa a ogni gruppo abeliano l'insieme dei suoi elementi e ad ogni omomorfismo la mappa insiemistica soggiacente.

D viene chiamato *funtore dimenticante* (forgetful functor), proprio perché quello che fa è "dimenticare" la struttura di gruppo. Quello che vorremmo mostrare ora è che

Proposizione 7.29. $D \circ \mathrm{Ext}^1$ è naturalmente equivalente ad E.

Non lo mostreremo per davvero: ci accontenteremo di mostrare l'isomorfismo sugli oggetti il che, visto che stiamo parlando di funtori in Set, vuol dire mostrare che per ogni A, B esiste una bigezione fra $D \circ \mathrm{Ext}^1(A, B)$ e $E(A, B)$. Cominciamo fissando una presentazione proiettiva di A

$$0 \to R \xrightarrow{\mu} P \xrightarrow{\epsilon} A \to 0$$

e associando ad ogni estensione $0 \to B \to E \to A \to 0$ un elemento $[\psi] \in \mathrm{Hom}(R, B)/\operatorname{Im} T\mu \cong \mathrm{Ext}^1(A, B)$. Consideriamo il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & & & \vdots{\scriptstyle \pi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

dove π esiste per proiettività di P. A questo punto, dato che κ è iniettiva, vorremmo usare κ^{-1} per arrivare in B. Il problema è che κ^{-1} non è definita su tutto E, ma solo su $\operatorname{Im}\kappa$; tuttavia, per esattezza e commutatività,

$$\nu \circ \pi \circ \mu = \mathrm{id}_A \circ \epsilon \circ \mu = \mathrm{id}_A \circ 0 = 0$$

per cui $\operatorname{Im}\pi \circ \mu \subseteq \operatorname{Ker}\nu = \operatorname{Im}\kappa$ e ha senso porre $\psi = \kappa^{-1} \circ \pi \circ \mu$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \pi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

Ora ψ dipende dalla scelta di π, ma $[\psi]$ no, che è quello che ci interessa. Infatti se π' è un altro sollevamento analogamente a prima abbiamo $\operatorname{Im}(\pi' - \pi) \subset \operatorname{Ker}\nu = \operatorname{Im}\kappa$, per cui per proiettività di P esiste τ tale che $\pi' - \pi = \kappa \circ \tau$, e dato che $(\pi' - \pi) \circ \mu = \kappa \circ (\psi' - \psi)$, si ha anche $\psi' - \psi = \kappa^{-1} \circ (\pi' - \pi) \circ \mu = \tau \circ \mu$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi' - \psi} & \swarrow{\scriptstyle \tau} & \downarrow{\scriptstyle \pi' - \pi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

e il fatto che esista τ tale che $\psi' - \psi = \tau \circ \mu$ per definizione vuol dire che $\psi' - \psi \in \operatorname{Im} T\mu$, e quindi $[\psi'] = [\psi]$.

Mostriamo che $[\psi]$ non dipende dal rappresentante scelto per la classe di equivalenza di estensioni. Mettiamoci nella situazione in figura:

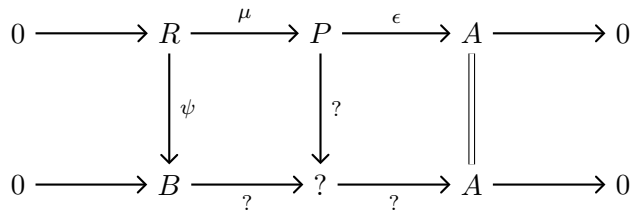
$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \pi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \vartheta} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\widetilde{\kappa}]{} & \widetilde{E} & \xrightarrow[\widetilde{\nu}]{} & A & \longrightarrow & 0 \end{array}$$

Visto che sappiamo che $[\psi]$ non dipende dal sollevamento scelto, calcoliamo $\widetilde{\psi}$ per l'estensione in basso usando il sollevamento $\widetilde{\pi} = \vartheta \circ \pi$. Per commutatività del diagramma sopra abbiamo[15]

$$\widetilde{\psi} = (\widetilde{\kappa})^{-1} \widetilde{\pi} \mu = (\vartheta\kappa)^{-1} \vartheta\pi\mu = \kappa^{-1}\vartheta^{-1}\vartheta\pi\mu = \kappa^{-1}\pi\mu = \psi$$

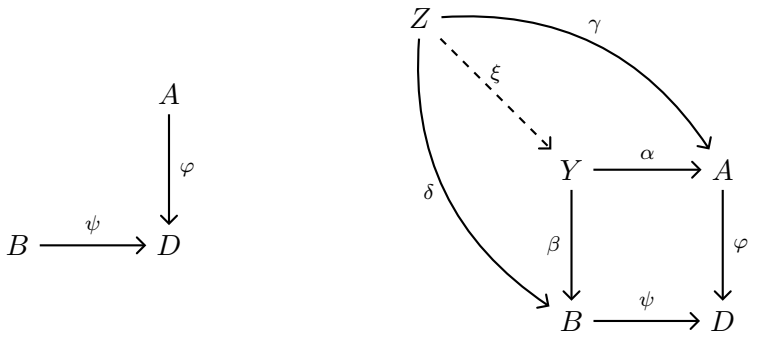
[15] Per convincersi potrebbe bastare leggere la prima uguaglianza seguendola "col dito" sul diagramma.

Per mostrare che questa mappa è bigettiva vogliamo esibirne l'inversa: data $[\psi]$ vorremmo ottenere un'estensione di A tramite B completando il seguente diagramma

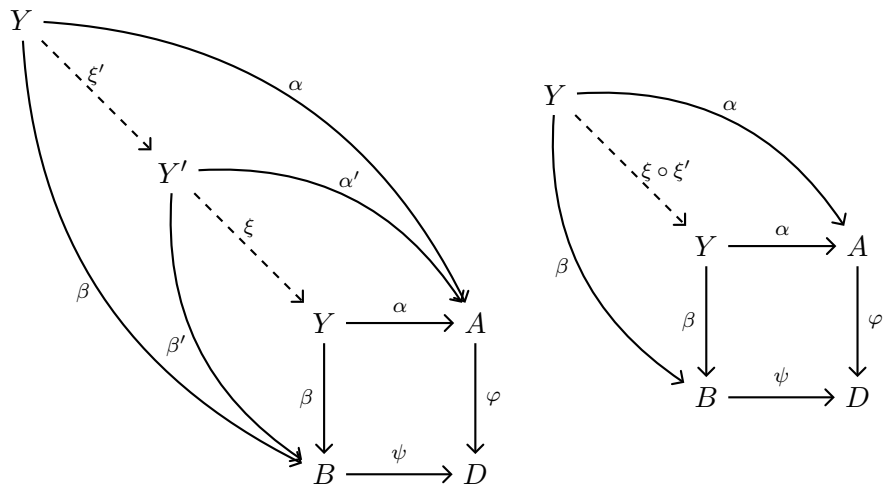


Ora, noi stiamo "barando", nel senso che non verificheremo la naturale equivalenza fra $D \circ \mathrm{Ext}^1$ ed E, ma il lettore dovrebbe essersi accorto che, a livello di euristica, per far venire fuori una trasformazione naturale la prima cosa che si prova a fare è usare costruzioni "naturali", "universali" o "le prime che ci vengono in mente", nel senso che devono essere le "più piccole" (in un qualche senso) che fanno commutare i diagrammi, come il prodotto diretto. La "prima cosa che ci viene in mente" in questo caso si chiama *pushout*, ma vediamo prima la nozione duale:

Definizione 7.30. Date due mappe φ, ψ come nel diagramma a sinistra il loro *pullback* è dato da Y, α e β tali che nel diagramma a destra il quadrato commuti e per ogni Z, γ, δ come nel diagramma esiste un'unica ξ che continui a farlo commutare.

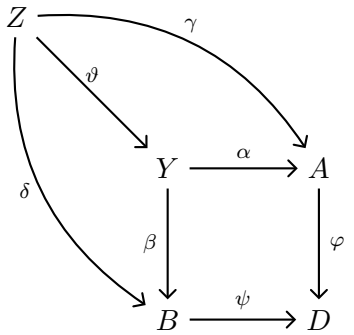


Come per tutte le "costruzioni universali" — ad esempio il prodotto — se Y esiste è unico a meno di isomorfismo. Visto che non abbiamo mai visto come si dimostra — ad esempio per il prodotto — ma l'idea è sempre la stessa, vediamolo per il pullback. Il trucco è prendere un altro pullback Y', con le sue mappe α', β', e invocare la proprietà di pullback sia su Y che su Y' disegnando il diagramma a sinistra:



A questo punto $\xi \circ \xi'$ va bene come mappa che realizza la proprietà di pullback di Y nel diagramma a destra, ma dato che anche id_Y andrebbe bene e che nella definizione di pullback la "mappa che va bene" è unica abbiamo $\xi \circ \xi' = \mathrm{id}_Y$. Ripetendo il ragionamento scambiando i ruoli di Y e Y' otteniamo $\xi' \circ \xi = \mathrm{id}_{Y'}$, e quindi Y e Y' sono isomorfi. Non solo: di isomorfismi come ξ, cioè che facciano commutare la parte interna del diagramma a sinistra, ce n'è solo uno, perché l'abbiamo trovato invocando la proprietà di pullback.

Osservazione 7.31. Se Y, α, β sono un pullback di φ e ψ e abbiamo un diagramma commutativo del tipo



allora per dimostrare che Z, γ, δ sono un pullback di φ e ψ basta verificare che ϑ sia un isomorfismo.

Dimostrazione. Per verificare la proprietà di pullback per Z basta sfruttare quella di Y passando da ϑ (e dato che il diagramma commuta le mappe sono proprio γ e δ). □

Il pullback viene anche chiamato *prodotto fibrato* per ragioni geometriche.

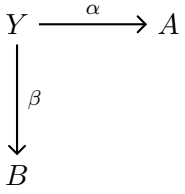
Nella categorie $\mathscr{M}_\Lambda$ il pullback esiste sempre: si considera la mappa

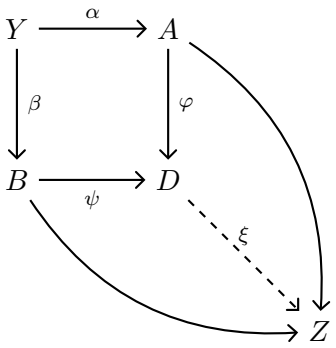
$$\langle \varphi, -\psi \rangle \colon A \oplus B \to D \qquad \langle \varphi, -\psi \rangle (a, b) = \varphi(a) - \psi(b)$$

e si pone[16] $Y = \operatorname{Ker}\langle \varphi, -\psi \rangle$, $\alpha = (\pi_A)_{\restriction Y}$ e $\beta = (\pi_B)_{\restriction Y}$.

Definizione 7.32. Il *pushout* è il pullback in $\mathcal{C}^{\mathrm{op}}$.

Dato che col pushout ci dobbiamo lavorare (e ci vogliamo anche fare esplicitamente qualche conto) sarà meglio vedere la definizione esplicita e disegnare qualche diagramma: il pushout di quello a sinistra è dato da D, φ, ψ tali che per ogni Z e frecce come nel diagramma a destra esiste un'unica ξ che continua a farlo commutare:

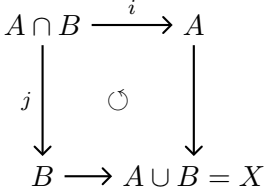




Anche il pushout è unico a meno di isomorfismo — esattamente per "lo stesso" motivo del pullback[17] — e nelle categorie $\mathscr{M}_\Lambda$ esiste sempre, ed è[18] $\operatorname{Coker}\langle \alpha, -\beta \rangle$ con le inclusioni passate al quoziente:

$$D = \frac{A \oplus B}{\operatorname{Im}\langle \alpha, -\beta \rangle} \qquad \varphi = [i_A]_{\operatorname{Im}\langle \alpha, -\beta \rangle} \qquad \psi = [i_B]_{\operatorname{Im}\langle \alpha, -\beta \rangle}$$

Un pushout famoso è quello che salta fuori quando si hanno $X = A \cup B$ spazi topologici *belli*[19], con $A \cap B$ connesso per archi e vari punti base che non scriviamo. Qui abbiamo



Applicando il funtore π_1, otteniamo il seguente diagramma in Grp

[16] Le verifiche possono essere reperite in [4] a pagina 35.
[17] Vedi Esercizio A.16.
[18] Vedi sempre [4], pagina 37.
[19] Connessi, localmente connessi per archi...

$$\begin{array}{ccc} \pi_1(A \cap B) & \xrightarrow{i^*} & \pi_1(A) \\ \Big\downarrow{\scriptstyle j^*} & & \\ \pi_1(B) & & \end{array}$$

e il pushout che completa il quadrato è proprio il prodotto amalgamato

$$\frac{\pi_1(A) * \pi_1(B)}{\langle i_*(a) j_*(a)^{-1} \rangle}$$

In altre parole una maniera molto stringata di enunciare il Teorema di Van Kampen è "il π_1 porta pushout in pushout".

I pullback/pushout non esistono in tutte le categorie. Basta considerare il poset con tre elementi a, b, c e relazioni $a \leq b$, $a \leq c$: qui semplicemente non c'è nessun $d \geq b, c$ che possa "completare il quadrato" a pushout. Anche se il quadrato si può completare non è detto che lo si possa fare con un elemento "minimo": si prenda l'esempio di prima aggiungendo una copia di $\mathbb{Z}$ maggiore di $a, b, c \ldots$ Qualche esempio di carattere più algebrico: la categoria dei moduli liberi su un qualsiasi anello non ammette pushout, e la categoria dei moduli finitamente generati su un anello non noetheriano non ammette pullback.

Per usare i pushout per costruire estensioni di moduli ci servono un paio di risultati, che enunciamo e dimostriamo per i pullback, ma che possono essere dualizzati[20]. Si veda l'Esercizio A.16.

Lemma 7.33. Se il quadrato qui sotto è un pullback di Λ-moduli

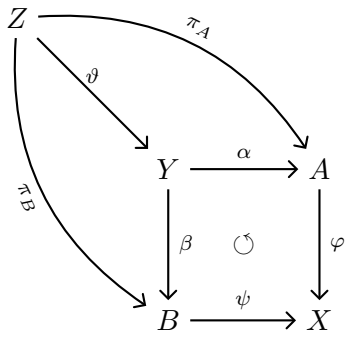
$$\begin{array}{ccc} Y & \xrightarrow{\alpha} & A \\ \Big\downarrow{\scriptstyle \beta} & \circlearrowleft & \Big\downarrow{\scriptstyle \varphi} \\ B & \xrightarrow{\psi} & X \end{array}$$

allora β induce un isomorfismo fra $\operatorname{Ker} \alpha$ e $\operatorname{Ker} \psi$.

Dimostrazione. Consideriamo il pullback "costruito a mano" presentato poco fa, cioè $Z = \operatorname{Ker}\langle \varphi, -\psi \rangle$, dove $\langle \varphi, -\psi \rangle \colon A \oplus B \to X$ è la mappa $(a, b) \mapsto \varphi(a) - \psi(b)$. Per la proprietà di pullback applicata a Y esiste ϑ che fa commutare il diagramma sotto, e dato che anche Z è un pullback ϑ è un isomorfismo[21].

[20] ... e che useremo proprio nella versione duale.

[21] Se non è chiaro perché si riveda la dimostrazione dell'unicità dei pullback poco indietro.



Per commutatività ϑ induce[22] un isomorfismo fra $\operatorname{Ker}\pi_A$ e $\operatorname{Ker}\alpha$. Inoltre

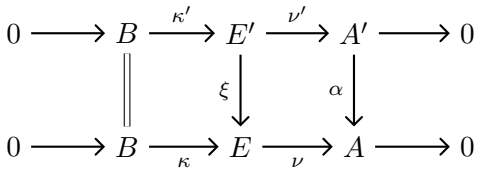
$$\operatorname{Ker}\pi_A = Z \cap \{(0,b) \mid b \in B\} = \{(0,b) \mid b \in \operatorname{Ker}\psi\}$$

Da questo è immediato vedere che $\pi_{B\restriction \operatorname{Ker}\pi_A}$ è sia iniettiva che surgettiva su $\operatorname{Ker}\psi$, quindi è un isomorfismo, e per avere la tesi basta comporre

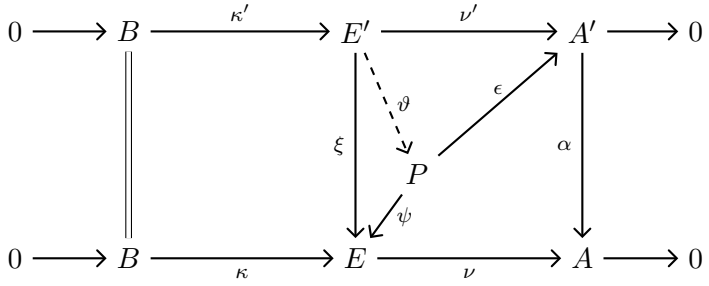
$$\operatorname{Ker}\alpha \xrightarrow{(\vartheta_{\restriction \operatorname{Ker}\alpha})^{-1}} \operatorname{Ker}\pi_A \xrightarrow{\pi_B} \operatorname{Ker}\psi \qquad \square$$

Ora impariamo a "riconoscere un pullback":

Lemma 7.34. In un diagramma commutativo a righe esatte come sotto il quadrato a destra è un pullback, cioè E', ν' e ξ sono il pullback di α e ν.



Dimostrazione. Inseriamo nel diagramma un pullback di α e ν con la mappa data dalla sua proprietà universale (quella tratteggiata):



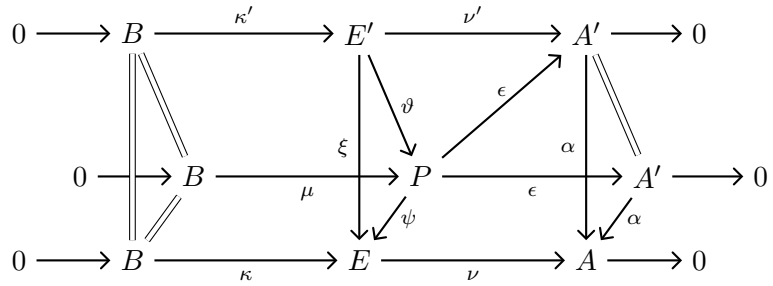
Il diagramma sopra continua a commutare per definizione di pullback quindi, se mostriamo che ϑ è un isomorfismo, per l'Osservazione 7.31 abbiamo finito.

[22] Nel senso che la sua restrizione a $\operatorname{Ker}\pi_A$ è l'isomorfismo cercato.

Usando l'isomorfismo del Lemma precedente e sfruttando l'esattezza della riga inferiore del diagramma troviamo un isomorfismo

$$\operatorname{Ker}\epsilon \xrightarrow{\psi_{\restriction \operatorname{Ker}\epsilon}} \underbrace{\operatorname{Ker}\nu}_{=\operatorname{Im}\kappa} \xrightarrow{(\kappa_{\restriction \operatorname{Ker}\nu})^{-1}} B$$

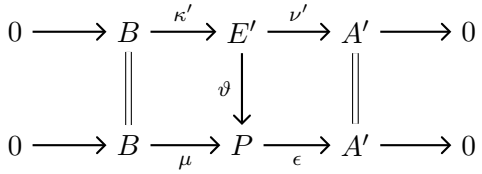
Se $\mu\colon B \to \operatorname{Ker}\epsilon$ è l'inversa di tale isomorfismo per la riga sopra $\psi_{\restriction \operatorname{Ker}\epsilon} \circ \mu = \kappa$, per cui possiamo aggiungere al diagramma un'altra riga esatta:



In questo diagramma gli unici quadrati "veramente" nuovi sono i due a sinistra che coinvolgono μ, e abbiamo verificato che quello in basso commuta prima ancora di disegnarlo. Verifichiamo che anche il quadrato in alto a sinistra commuta, cioè che $\vartheta \circ \kappa' = \mu$. Dato che $\epsilon \circ \vartheta \circ \kappa' = \nu' \circ \kappa' = 0$ abbiamo $\operatorname{Im}\vartheta \circ \kappa' \subseteq \operatorname{Ker}\epsilon$, e quindi

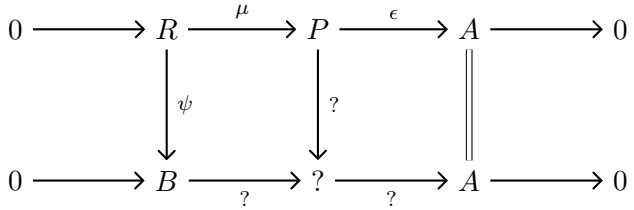
$$\psi_{\restriction \operatorname{Ker}\epsilon} \circ \vartheta \circ \kappa' = \xi \circ \kappa' = \kappa = \psi_{\restriction \operatorname{Ker}\epsilon} \circ \mu$$

Ma dato che $\psi_{\restriction \operatorname{Ker}\epsilon}$ è un isomorfismo $\vartheta \circ \kappa' = \mu$, come voluto. Facendo "pulizia" cancellando la riga inferiore e tutto ciò che la coinvolge troviamo il diagramma commutativo a righe esatte



e per la Proposizione 6.9 ϑ è un isomorfismo. □

Torniamo al problema iniziale: volevamo associare un'estensione di A tramite B a $[\psi] \in \operatorname{Hom}(R, B)/\operatorname{Im} T\mu$ completando il seguente diagramma



Inseriamo il pushout di μ e ψ nel diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\beta]{} & \frac{B\oplus P}{\mathrm{Im}\langle\psi,-\mu\rangle} & & A & \longrightarrow & 0 \end{array}$$

Per il duale del Lemma 7.33 α induce un isomorfismo fra Coker β e Coker $\mu \cong A$, quindi abbiamo il diagramma commutativo a righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\beta]{} & \frac{B\oplus P}{\mathrm{Im}\langle\psi,-\mu\rangle} & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

Dove ν fa commutare il quadrato a destra per "lo stesso" motivo[23] per cui la μ del Lemma 7.34 faceva commutare quello a sinistra del relativo diagramma. Dato che la riga di sotto è esatta abbiamo effettivamente fra le mani un'estensione di A tramite B, e ci resta solo da verificare che la sua classe di equivalenza non dipende dal rappresentate scelto per $[\psi]$. Se $[\psi] = [\psi']$ allora $\psi' = \psi + \tau \circ \mu$, e dato che

$$\beta\psi' = \beta(\psi + \tau\mu) = \beta\psi + \beta\tau\mu = \alpha\mu + \beta\tau\mu = (\alpha + \beta\tau)\mu$$

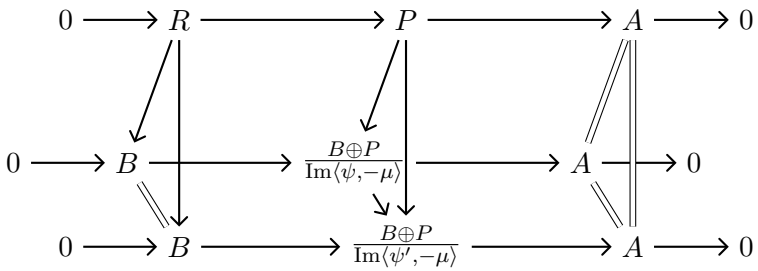
otteniamo un diagramma commutativo[24] a patto di aggiungere $\beta\tau$ ad α:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi+\tau\mu} & \swarrow{\scriptstyle \tau} & \downarrow{\scriptstyle \alpha+\beta\tau} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\beta]{} & \frac{B\oplus P}{\mathrm{Im}\langle\psi,-\mu\rangle} & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

e per il duale del Lemma precedente il quadrato a sinistra è un pushout. Ne segue che l'estensione costruita con ψ' è equivalente a quella costruita con ψ, per essenzialmente lo stesso discorso che mostra l'unicità dei pushout più la Proposizione 6.9 applicati al diagramma

[23] Non me la sono proprio sentita di scrivere "il motivo duale". Al lettore poco convinto non resta che provare a dualizzare il Lemma 7.34.

[24] Modulo la freccia a zigzag.



e abbiamo costruito l'inversa cercata[25]. Il lettore interessato alla dimostrazione che $D \circ \mathrm{Ext}^1$ ed E sono naturalmente equivalenti può consultare [4] a pagina 54.

7.5 Calcolo di Alcuni Ext

Notazione 7.35. Indicheremo $\mathbb{Z}/n\mathbb{Z}$ con $\mathbb{Z}_n$. In tutta la sezione lavoriamo su $\mathbb{Z}$, per cui Ext^1 vuol dire $\mathrm{Ext}^1_{\mathbb{Z}}$, Hom vuol dire $\mathrm{Hom}_{\mathbb{Z}}$, eccetera.

Calcoliamo $\mathrm{Ext}^1(\mathbb{Z}_4, \mathbb{Z}_4)$. Prendiamo la presentazione proiettiva

$$0 \to \mathbb{Z} \xrightarrow{\cdot 4} \mathbb{Z} \to \mathbb{Z}_4 \to 0$$

ci applichiamo $\mathrm{Hom}(-, \mathbb{Z}_4)$

$$0 \to \mathrm{Hom}\left(\mathbb{Z}_4, \mathbb{Z}_4\right) \to \mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}_4\right) \xrightarrow{(\cdot 4)^*} \mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}_4\right)$$

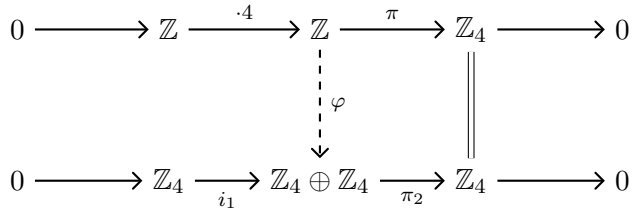
e quindi

$$\mathrm{Ext}^1\left(\mathbb{Z}_4, \mathbb{Z}_4\right) = \frac{\mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}_4\right)}{\mathrm{Im}(\cdot 4)^*} \cong \frac{\mathbb{Z}_4}{(0)} \cong \mathbb{Z}_4$$

Vediamo chi sono questi quattro elementi. L'estensione banale, che spezza,

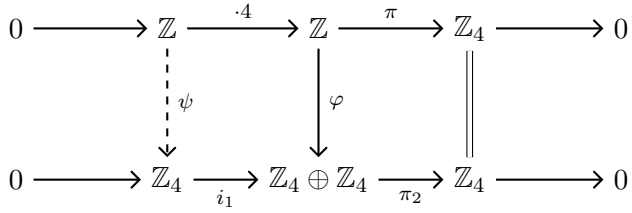
$$0 \to \mathbb{Z}_4 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4 \to \mathbb{Z}_4 \to 0$$

è quella che corrisponde a 0. Infatti, se disegniamo



possiamo scegliere come sollevamento $\varphi(n) = (0, [n]_4)$. Quando andiamo a sollevare a ψ

[25] La verifica che le due mappe esibite sono inverse l'una dell'altra può essere reperita in [4] a pagina 56.

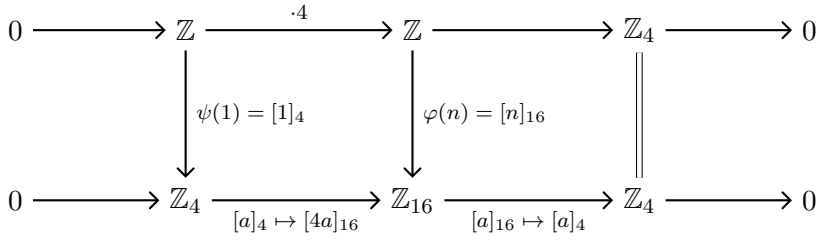


deve valere $\varphi(4n) = i_1 \circ \psi(n)$, cioè $(0,0) = \varphi(4n) = (\psi(n), 0)$, e quindi $\psi = 0$.

Un'altra estensione è

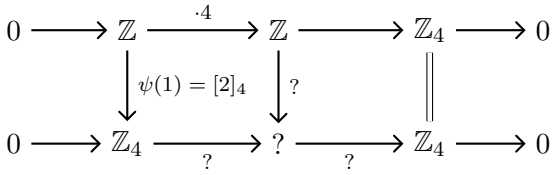
$$0 \to \mathbb{Z}_4 \xrightarrow{[a]\mapsto[4a]} \mathbb{Z}_{16} \to \mathbb{Z}_4 \to 0$$

Sollevando si trova



dunque ψ è l'omomorfismo associato a $[1]$. Ce ne mancano due.

Questa volta invece di partire da un oggetto noto partiamo dall'omomorfismo $\psi = 2$, cioè quello che manda 1 in $[2]_4$, e calcoliamo il pushout



Dato che $\mathrm{Im}\langle \cdot 4, -\psi\rangle = \langle (4, -[2]_4)\rangle = \langle (4, [2]_4)\rangle$ il nostro uomo è

$$\frac{\mathbb{Z} \oplus \mathbb{Z}_4}{\langle (4, [2]_4)\rangle} \cong \frac{\mathbb{Z} \oplus \mathbb{Z}}{\langle (0,4), (4,2)\rangle}$$

e per capire chi è il signore a destra invochiamo la Forma di Smith:

$$\begin{pmatrix} 4 & 0 \\ 2 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 4 & -8 \\ 2 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -8 \\ 2 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}$$

e dunque il signore in questione è[26] $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Per $\psi = 3$, anche se non vediamo il conto, l'oggetto nel centro dell'estensione viene sempre $\mathbb{Z}/16\mathbb{Z}$,

[26] Le mappe possono essere ricavate "tracciando" i vari isomorfismi usati, incluse le mosse usate per il calcolo della Forma di Smith, o imponendo che il diagramma commuti.

ma quest'estensione *non* è isomorfa a quella per $\psi = 1$, perché sappiamo che l'Ext^1 classifica le estensioni a meno di isomorfismo. La mappa, se prima era la $\cdot 4$, questa volta è la $\cdot 12$. In altre parole non ci sono mappe che completano il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_4 & \xrightarrow{a \mapsto [4a]} & \mathbb{Z}_{16} & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 \\ & & \| & & & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_4 & \xrightarrow{a \mapsto [16a]} & \mathbb{Z}_{16} & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 \end{array}$$

e il concetto di estensione è profondamente legato alle mappe e *non solo* agli oggetti. Calcoliamo un altro Ext^1.

Esercizio 7.36. Calcolare $\mathrm{Ext}^1(\mathbb{Z}_{36}, \mathbb{Z}_{42})$ e, per ogni suo elemento, indicare l'estensione associata.

Soluzione. Calcoliamo, in generale, $\mathrm{Ext}^1(\mathbb{Z}_n, \mathbb{Z}_m)$. Prendiamo la presentazione proiettiva di $\mathbb{Z}_n$

$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}_n \to 0$$

applichiamo il funtore $\mathrm{Hom}(-, \mathbb{Z}_m)$ e otteniamo

$$0 \to \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \to \underbrace{\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_m)}_{\cong \mathbb{Z}_m} \xrightarrow{(\cdot n)^*} \underbrace{\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_m)}_{\cong \mathbb{Z}_m}$$

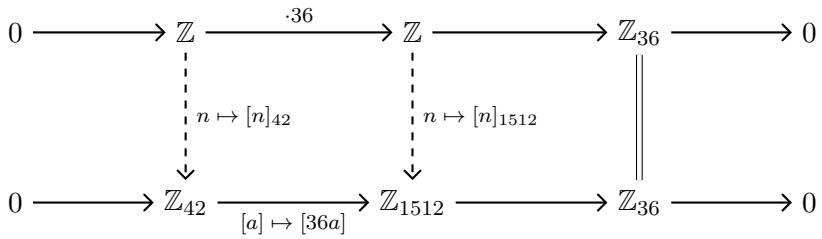
Dunque abbiamo

$$\mathrm{Ext}^1(\mathbb{Z}_n, \mathbb{Z}_m) \cong \frac{\mathbb{Z}_m}{\langle [n]_m \rangle} \cong \mathbb{Z}_{\gcd(n,m)}$$

Nel nostro caso particolare, dunque, $\mathrm{Ext}^1(\mathbb{Z}_{36}, \mathbb{Z}_{42}) \cong \mathbb{Z}_6$. Ora però vogliamo capire come sono fatte queste 6 estensioni. Come prima (e come sempre, con la stessa dimostrazione) lo 0 corrisponde all'estensione "split"

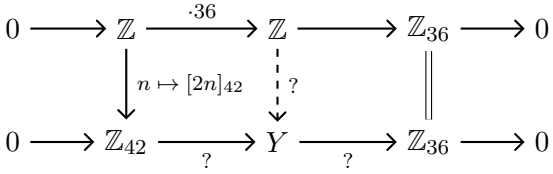
$$0 \to \mathbb{Z}_{42} \to \mathbb{Z}_{42} \oplus \mathbb{Z}_{36} \to \mathbb{Z}_{36} \to 0$$

Capiamo a chi corrisponde $[1] \in \mathbb{Z}_6 = \mathrm{Ext}^1(\mathbb{Z}_{36}, \mathbb{Z}_{42})$. Questa volta invece di usare il pushout proviamo a sollevare l'identità, cioè a "indovinare" mettendo le prime mappe sensate che ci vengono in mente. Il diagramma è $(36 \cdot 42 = 1512)$



e dato che commuta siamo "stati fortunati" e l'estensione è proprio quella.

Il [2] facciamolo per benino, ossia coi pushout:



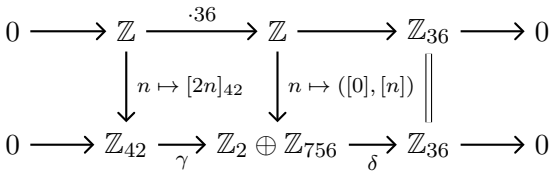
Sappiamo che deve essere $Y = (\mathbb{Z} \oplus \mathbb{Z}_{42})/(\mathrm{Im}\langle \cdot 36, -[2n] \rangle)$; ricordiamo che la grafia con $\langle -, - \rangle$ vuol dire che mappiamo

$$\mathbb{Z} \ni n \mapsto (36n, -[2n]_{42}) \in \mathbb{Z} \oplus \mathbb{Z}_{42}$$

comunque viene $Y = (\mathbb{Z} \oplus \mathbb{Z})/\langle (0, 42), (36, -2) \rangle$, e la matrice che salta fuori e la sua forma di Smith sono (passaggi non riportati)

$$\begin{pmatrix} 0 & 36 \\ 42 & -2 \end{pmatrix} \cong \begin{pmatrix} 2 & 0 \\ 0 & 756 \end{pmatrix}$$

e quindi l'estensione è



dove per capire chi è la mappa γ bisognerebbe "seguirla attraverso il cambio di base" che abbiamo fatto per mettere la matrice in forma di Smith, o alternativamente si può imporre che il diagramma commuti. Comunque facendo i conti si ha $\gamma = [n] \mapsto [([n]_2, [36 \cdot 11n]_{756})$, mentre δ è la mappa che manda $([1], [0]) \mapsto [0]_{36}$ e $([0], [1]) \mapsto [1]_{36}$.

Trovare le altre estensioni per esercizio. Per quelli che veramente proseguono, la corrispondenza è

$$[3] \mapsto \mathbb{Z}_3 \oplus \mathbb{Z}_{504} \qquad [4] \mapsto \mathbb{Z}_2 \oplus \mathbb{Z}_{756} \qquad [5] \mapsto \mathbb{Z}_{1512}$$

e anche questa volta le estensioni sono a due a due non equivalenti, anche nel caso in cui i loro E siano moduli isomorfi. □

Osservazione 7.37. $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}_m) = 0$ e $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}) = 0$

Questo è facile da vedere, perché $\mathbb{Z}$ è libero e in particolare proiettivo, dunque l'unica estensione è quella che spezza. Alternativamente si può fare il conto dell'Ext^1 con la presentazione proiettiva

$$0 \to 0 \to \mathbb{Z} \to \mathbb{Z} \to 0$$

Se poi la allunghiamo con un bel po' di zeri a sinistra otteniamo una risoluzione proiettiva abbastanza banale, da cui segue per ogni $n \geq 1$, $\mathrm{Ext}^n(\mathbb{Z}, A) = 0$. Suona familiare? Effettivamente l'avevamo già detto (Proposizione 7.20).

Esattamente nella stessa maniera si mostra che se A è libero $\mathrm{Ext}(A, \mathbb{Z}) = 0$. È vero il viceversa?

Dato che $\mathrm{Ext}(\mathbb{Z}_m, \mathbb{Z}) \cong \mathbb{Z}_m$ e $\mathrm{Ext}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_{\gcd(n,m)}$, *se A è un gruppo abeliano finitamente generato*, per il relativo Teorema di Struttura A è libero se e solo se $\mathrm{Ext}(A, \mathbb{Z}) = 0$, perché $\mathrm{Ext}(\oplus A_i, B) \cong \prod \mathrm{Ext}(A_i, B)$.

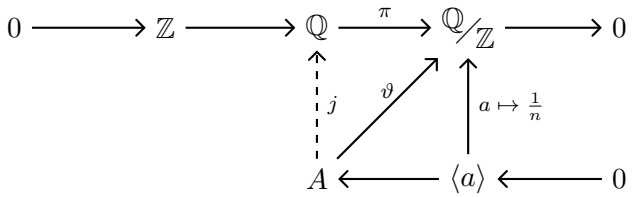
Tolta l'ipotesi di finita generatezza chiedersi se $\mathrm{Ext}(A, \mathbb{Z}) = 0$ implica A libero è un questione sufficientemente delicata da essersi meritata un nome: *problema di Whitehead*. Serre ha mostrato che è vero se A è numerabilmente generato, mentre in generale l'esistenza di *gruppi di Whitehead* — cioè di $\mathbb{Z}$-moduli A tali che $\mathrm{Ext}(A, \mathbb{Z}) = 0$ — che non siano liberi è indipendente[27] da ZFC.

Esercizio 7.38. Se A è un gruppo abeliano con torsione $\overline{\mathrm{Ext}}^1(A, \mathbb{Z}) \neq 0$.

Soluzione. Risolviamo iniettivamente[28] $\mathbb{Z}$:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \to 0 \to \cdots$$

Sia $a \in A$ un elemento di n-torsione. Per iniettività di $\mathbb{Q}/\mathbb{Z}$ possiamo estendere la mappa $a \mapsto 1/n$ ad una ϑ definita su tutto A



[27] Qualche dettaglio in più per gli appassionati di Teoria degli Insiemi: Shelah ha mostrato in [18] che sotto $V = L$ ogni gruppo di Whitehead è libero, mentre sotto MA+¬CH esistono gruppi di Whitehead non liberi. Successivamente, in [19] e [20], sempre Shelah ha mostrato che possono esistere gruppi di Whitehead non liberi anche in presenza di CH.

[28] Vedi Fatto 7.24.

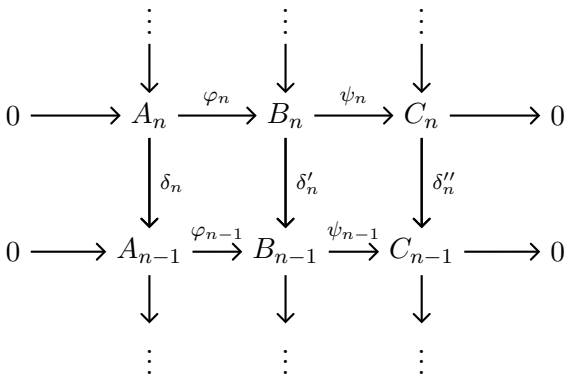
Ora una qualunque j come nel diagramma deve per forza mandare a in 0 ($\mathbb{Q}$ non ha torsione), e quindi ϑ non appartiene all'immagine di π_*, per cui

$$\overline{\mathrm{Ext}}^1(A,\mathbb{Z}) = \frac{\overbrace{\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})}^{=\mathrm{Ker}\to 0}}{\mathrm{Im}\,\pi^*} \neq 0$$

□

7.6 Successioni Esatte Lunghe

Teorema 7.39. Sia $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ una successione esatta corta in Comp_Λ, cioè un diagramma commutativo a righe esatte del tipo



Allora esiste un omomorfismo di moduli graduati ω di grado -1 tale che

$$\cdots \xrightarrow{\omega_{n+1}} H_n(A) \xrightarrow{(\varphi_*)_n} H_n(B) \xrightarrow{(\psi_*)_n} H_n(C) \xrightarrow{\omega_n} H_{n-1}(A) \to \cdots$$

è esatta.

Dimostrazione. L'omomorfismo ω è definito più o meno come nel Lemma del Serpente. Prendiamo $[c]_{\mathrm{Im}\,\delta''_{n+1}} \in H_n(C)$, rappresentato da $c \in \mathrm{Ker}\,\delta''_n$. Per surgettività esiste $b \in B_n$ tale che $c = \psi_n(b)$, da cui per commutatività

$$0 = \delta''_n(c) = \delta''_n(\psi_n(b)) = \psi_{n-1}\delta'_n(b)$$

dunque $\delta'_n(b) \in \mathrm{Ker}\,\psi_{n-1} = \mathrm{Im}\,\varphi_{n-1}$ per esattezza, per cui esiste a tale che $\delta'_n(b) = \varphi_{n-1}(a)$, e dato che φ_{n-1} è iniettiva possiamo porre

$$\omega_n(\overline{c}) = [\varphi_{n-1}^{-1}(\delta'_n(b))]_{\mathrm{Im}\,\delta_n}$$

Dopodiché c'è da verificare che la definizione non dipende dalle scelte fatte, cioè dal rappresentante c né dal b tale che $c = \psi_n(b)$, e che effettivamente ω_n rende la successione esatta[29]. □

[29] Questa cosa viene generalmente lasciata come esercizio, ma il lettore pigro può trovare tutti i dettagli su [4] a pagina 74.

Il Teorema 7.39 ha la seguente conseguenza sui funtori derivati:

Proposizione 7.40 (Prima successione esatta lunga dei funtori derivati)**.** Sia F un funtore additivo, L_iF i suoi funtori derivati e $0 \to A \to B \to C \to 0$ esatta. Allora c'è una successione esatta lunga

$$\cdots \to L_nFA \to L_nFB \to L_nFC \to L_{n-1}FA \to \cdots$$
$$\cdots \to L_1FC \to L_0FA \to L_0FB \to L_0FC \to 0$$

Ovviamente se F è esatto a destra ci si può dimenticare degli L_0 e scrivere F invece di L_0F, per gli stessi motivi dell'Osservazione 7.18.

Dimostrazione. Prendiamo una risoluzione libera di A e una di C

$$\cdots \to S_2 \to S_1 \to S_0 \to A \to 0$$
$$\cdots \to T_2 \to T_1 \to T_0 \to C \to 0$$

costruiamo per B una risoluzione "furba". Disegniamo il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S_0 & \xrightarrow{i} & S_0 \oplus T_0 & \xrightarrow{\pi} & T_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow[\varphi]{} & B & \xrightarrow[\psi]{} & C & \longrightarrow & 0 \end{array}$$

per proiettività possiamo aggiungere u che fa commutare il triangolo a destra[30]

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S_0 & \xrightarrow{i} & S_0 \oplus T_0 & \xrightarrow{\pi} & T_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & & \swarrow{\scriptstyle u} & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow[\varphi]{} & B & \xrightarrow[\psi]{} & C & \longrightarrow & 0 \end{array}$$

e a questo punto definiamo $\beta(s,t) = \varphi \circ \alpha(s) + u(t)$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S_0 & \xrightarrow{i} & S_0 \oplus T_0 & \xrightarrow{\pi} & T_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & \swarrow{\scriptstyle u} & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow[\varphi]{} & B & \xrightarrow[\psi]{} & C & \longrightarrow & 0 \end{array}$$

[30] Occhio, non è detto che tutto il diagramma commuti: in generale $u \circ \pi \circ i = u \circ 0 \neq \varphi \circ \alpha$.

che fa commutare il diagramma[31] — basta pensarci un attimo — ed è surgettiva perché α, γ lo sono. Invocando il Lemma del Serpente abbiamo la successione esatta

$$\underbrace{\operatorname{Coker}\alpha}_{=0} \to \operatorname{Coker}\beta \to \underbrace{\operatorname{Coker}\gamma}_{=0}$$

Sempre per il Lemma del Serpente abbiamo la successione esatta

$$0 \to \operatorname{Ker}\alpha \to \operatorname{Ker}\beta \to \operatorname{Ker}\gamma \to 0$$

per cui possiamo ripetere il ragionamento ottenendo il diagramma commutativo a righe *e colonne* esatte

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S_1 & \longrightarrow & S_1 \oplus T_1 & \longrightarrow & T_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{Ker}\alpha & \longrightarrow & \operatorname{Ker}\beta & \longrightarrow & \operatorname{Ker}\gamma & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Iterando la costruzione otteniamo una risoluzione proiettiva $S \oplus T$ di B

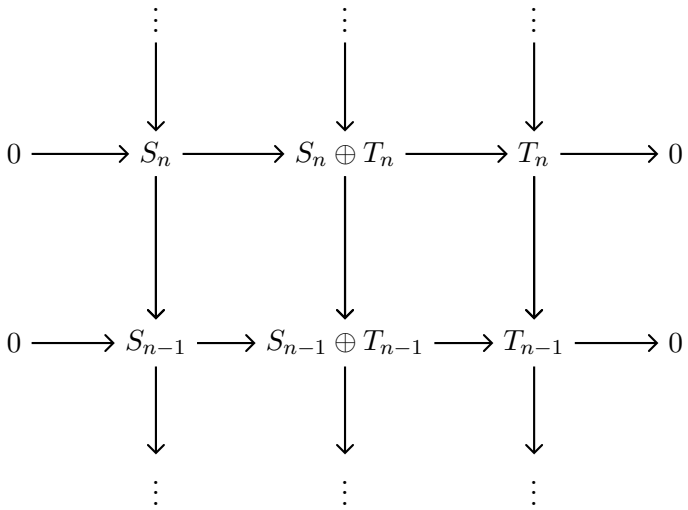
$$\cdots \to S_2 \oplus T_2 \to S_1 \oplus T_1 \to S_0 \oplus T_0 \to B \to 0$$

infatti

- Il complesso degli $S_n \oplus T_n$ è positivo per definizione
- Dato che ci siamo assicurati che l'ultima freccia (che non fa parte del complesso $S \oplus T$) sia surgettiva su B allora $H_0(S \oplus T) \cong B$.
- Dato che ci siamo assicurati che l'immagine di ogni altra freccia coincida col nucleo di quella dopo il complesso è aciclico.
- Ogni $S_n \oplus T_n$ è proiettivo in quanto somma di proiettivi.

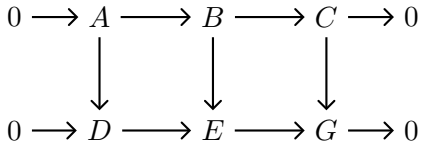
Inoltre abbiamo costruito la successione esatta corta di complessi

[31] Nel senso che i quadrati commutano, per u c'è sempre il problema di prima.



Ora ci si applica F e la successione del Teorema 7.39 è quella della tesi. Il fatto che le righe restino esatte è vero perché sono della forma $0 \to S \to S \oplus T \to T \to 0$ e F, in quanto additivo, porta somme dirette (finite) in somme dirette. Questo non l'abbiamo dimostrato, visto che non siamo andati nella direzione generale di lavorare in categorie additive[32] qualunque, comunque per i funtori che ci interessano, cioè Hom e $\otimes$, è palese. Per il caso generale si veda [6], Proposizione 9.5 del Capitolo II. □

La costruzione che abbiamo fatto è naturale, nel senso che se abbiamo



allora con le successioni esatte lunghe funziona tutto bene[33]. Questa proprietà quasi caratterizza i funtori derivati, nel senso che sono i funtori "minimali", in un qualche senso che qui non specifichiamo, che la verificano; anzi, in diversi testi la motivazione presentata per l'introduzione dei funtori derivati è proprio, dato un funtore T esatto — diciamo — a destra, prolungare verso sinistra la successione esatta data dall'esattezza a destra.

Come il lettore si aspetterà dal fatto che abbiamo parlato della *prima* successione esatta lunga, ce n'è anche una seconda:

[32]Nota per il lettore affamato di generalità: ad essere precisi per poter replicare le costruzioni viste finora l'ipotesi di essere in una categoria additiva non basta. Bisogna che Ker e Coker esistano e si comportino "bene", cosa che succede quando si lavora in categorie *abeliane*. Si veda la Sezione 9 del Capitolo II di [6].

[33]Per l'enunciato preciso si veda [6], Proposizione 6.2 del Capitolo IV.

Teorema 7.41 (Seconda successione esatta lunga per i funtori derivati)**.** Siano F, G, H funtori additivi con due trasformazioni naturali $F \xrightarrow{\varphi} G \xrightarrow{\psi} H$ tali che per ogni modulo M valga $\psi_M \circ \varphi_M = 0$ e per ogni modulo proiettivo[34] P la seguente successione sia esatta

$$0 \to FP \xrightarrow{\varphi_P} GP \xrightarrow{\psi_P} HP \to 0$$

Allora esistono dei morfismi $\delta_n \colon L_nHM \to L_{n-1}FM$ che rendono esatta

$$\cdots \xrightarrow{L_n\varphi_M} L_nGM \xrightarrow{L_n\psi_M} L_nHM \xrightarrow{\delta_n} L_{n-1}FM \xrightarrow{L_{n-1}\varphi_M} L_{n-1}GM \to \cdots$$
$$\xrightarrow{L_1\varphi_M} L_1GM \xrightarrow{L_1\psi_M} L_1HM \xrightarrow{\delta_1} L_0FM \xrightarrow{L_0\varphi_M} L_0GM \xrightarrow{L_0\psi_M} L_0HM \to 0$$

Anche qui se i funtori sono esatti a destra ci possiamo tranquillamente dimenticare gli L_0.

Dimostrazione. Prendiamo una risoluzione libera/proiettiva di M

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

Per ipotesi questa induce una successione esatta corta di complessi[35]

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & FP_1 & \xrightarrow{\varphi_{P_1}} & GP_1 & \xrightarrow{\psi_{P_1}} & HP_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & FP_0 & \xrightarrow{\varphi_{P_0}} & GP_0 & \xrightarrow{\psi_{P_0}} & HP_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

a cui basta applicare il Teorema 7.39 per avere la tesi. □

Anche questa volta la costruzione è naturale (nel senso di prima[36]).

7.7 Tor

Dati $M \in \mathscr{M}_\Lambda^r$ e $N \in \mathscr{M}_\Lambda^\ell$ consideriamo i funtori esatti a destra

$$F \equiv M \otimes_\Lambda - \colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab} \qquad G \equiv - \otimes_\Lambda N \colon \mathscr{M}_\Lambda^r \to \mathrm{Ab}$$

[34] Dovrebbe bastare libero.
[35] I quadrati commutano perché φ e ψ sono trasformazioni naturali.
[36] Anche questa volta l'enunciato preciso è su [6], Proposizione 6.4 del Capitolo IV.

Definiamo[37] $\overline{\mathrm{Tor}}_n(M,N) = L_nF(N)$ e $\mathrm{Tor}_n(M,N) = L_nG(M)$. Vedremo che $\mathrm{Tor}_n(M,N) \cong \overline{\mathrm{Tor}}_n(M,N)$. Prima, però, calcoliamo $\mathrm{Tor}_k(\mathbb{Z}_m,\mathbb{Z}_n)$ usando la risoluzione libera

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$\mathbb{Z}_m$$

Applichiamo $- \otimes_{\mathbb{Z}} \mathbb{Z}_n$ ottenendo il complesso

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}\otimes\mathbb{Z}_n \xrightarrow{\overbrace{\cdot m \otimes 1}^{=\mu}} \mathbb{Z}\otimes\mathbb{Z}_n \longrightarrow 0$$

da cui si ha subito

$$\begin{aligned}
&\mathrm{Tor}_k(\mathbb{Z}_m,\mathbb{Z}_n) = 0 \text{ per } k>1\\
&\mathrm{Tor}_1(\mathbb{Z}_m,\mathbb{Z}_n) = \operatorname{Ker}\mu\\
&\mathrm{Tor}_0(\mathbb{Z}_m,\mathbb{Z}_n) = \operatorname{Coker}\mu \cong \mathbb{Z}_m\otimes\mathbb{Z}_n
\end{aligned}$$

Ci resta quindi da capire chi è $\operatorname{Ker}\mu$. Dato che $\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}_n \cong \mathbb{Z}_n$ ci riduciamo a studiare il complesso

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}_n \xrightarrow{\cdot m} \mathbb{Z}_n \longrightarrow 0$$

e bisogna capire chi sono gli $x \in \mathbb{Z}_n$ tali che $mx \equiv 0 \pmod n$. Se $d = \gcd(m,n)$, $m = dm'$ e $n = dn'$ otteniamo $m'x \equiv 0 \pmod{n'}$, e dato che m' ed n' sono coprimi allora $x \equiv 0 \pmod{n'}$. Dunque[38]

$$\operatorname{Ker}\mu \cong \{x \in \mathbb{Z}_n \mid x \equiv 0 \pmod{n'}\} \cong \mathbb{Z}_d$$

In generale se A è un dominio commutativo con unità ed $f \neq 0$ possiamo calcolare $\mathrm{Tor}_1(A/(f),M)$, prendendo la risoluzione libera

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow A \xrightarrow{\cdot f} A \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$A/(f)$$

che è una risoluzione libera di $A/(f)$ perché per ipotesi A è un dominio e $f \neq 0$. Analogamente a prima consideriamo

[37] Occhio: precedentemente avevamo definito come Tor_n quello che ora si chiama $\overline{\mathrm{Tor}}_n$. Per evitare di riempire le pagine di $\overline{\ }$ si pensi alla notazione attuale come temporanea, finché non avremo mostrato l'equivalenza.

[38] Il fatto che $d = \gcd(m,n)$ sia simmetrico in m ed n ci piace, visto che vogliamo mostrare che il risultato è lo stesso anche con $\overline{\mathrm{Tor}}$.

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow A \otimes_A M \xrightarrow{\cdot f \otimes_A 1} A \otimes_A M \longrightarrow 0$$

e abbiamo

$$\begin{aligned}
&\mathrm{Tor}_k(A/(f), M) = 0 \text{ per } k > 1 \\
&\mathrm{Tor}_1(A/(f), M) = \{m \in M \mid fm = 0\} \\
&\mathrm{Tor}_0(A/(f), M) = A/(f) \otimes M \cong M/fM
\end{aligned}$$

Osservazione 7.42. Se $n > 0$ e M è proiettivo $\mathrm{Tor}_n(M, N) = 0$.

Dimostrazione. Basta prendere come risoluzione

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow M \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$M$$

□

Osservazione 7.43. Se $n > 0$ ed N è piatto allora $\mathrm{Tor}_n(M, N) = 0$.

Dimostrazione. Quando applichiamo $- \otimes_A N$ a una qualunque risoluzione, per piattezza otteniamo una successione esatta, che ha quindi omologia nulla[39]. □

Osservazione 7.44. Le due Osservazioni precedenti sono vere anche per[40] $\overline{\mathrm{Tor}}$, ma scambiando i ruoli di piatto e proiettivo.

Per la Proposizione 7.40 da una successione esatta

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

otteniamo la successione esatta lunga

$$\cdots \to \mathrm{Tor}_1(M_2, N) \to \mathrm{Tor}_1(M_3, N) \to M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

Inoltre, data una successione esatta $0 \to N_1 \to N_2 \to N_3 \to 0$ possiamo definire funtori e trasformazioni naturali come in figura

$$\underbrace{- \otimes N_1}_{F} \xrightarrow{\varphi} \underbrace{- \otimes N_2}_{G} \xrightarrow{\psi} \underbrace{- \otimes N_3}_{H}$$

e dato che proiettivo implica piatto, se P è proiettivo è esatta anche

$$0 \to P \otimes N_1 \to P \otimes N_2 \to P \otimes N_3 \to 0$$

[39] Tranne per l'H_0, ovviamente.

[40] Ed effettivamente una delle due cose l'avevamo già mostrata nella Proposizione 7.19, dove però $\overline{\mathrm{Tor}}_n$ si chiamava semplicemente Tor_n.

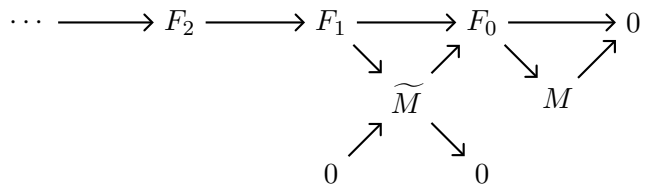
per cui possiamo usare il Teorema 7.41 e ottenere la successione esatta

$$\begin{aligned}\cdots \to \operatorname{Tor}_2(M,N_3) \to \operatorname{Tor}_1(M,N_1) \to \operatorname{Tor}_1(M,N_2) \to \\ \to \operatorname{Tor}_1(M,N_3) \to M\otimes N_1 \to M\otimes N_2 \to M\otimes N_3 \to 0\end{aligned}$$

Quanto sopra vale anche per $\overline{\operatorname{Tor}}$. Siamo pronti per dimostrare che

Teorema 7.45. $\operatorname{Tor}_k(M,N) \cong \overline{\operatorname{Tor}}_k(M,N)$.

Dimostrazione. Per induzione su k. Il caso $k=0$ è ovvio perché entrambi sono (naturalmente isomorfi a) $M\otimes N$. Per $k>0$ prendiamo una risoluzione libera di M e interrompiamola:



dunque abbiamo la successione esatta corta $0 \to \widetilde{M} \to F_0 \to M \to 0$, che induce l'esatta lunga

$$\cdots \to \underbrace{\operatorname{Tor}_1(F_0,N)}_{=0} \to \operatorname{Tor}_1(M,N) \to \widetilde{M}\otimes N \to F_0\otimes N \to M\otimes N \to 0$$

perché F_0 in quanto libero è proiettivo e si applica l'Osservazione 7.42. Analogamente, se $k\geq 2$, l'esattezza fornisce l'isomorfismo

$$0 = \operatorname{Tor}_k(F_0,N) \to \operatorname{Tor}_k(M,N) \xrightarrow{\cong} \operatorname{Tor}_{k-1}(\widetilde{M},N) \to \operatorname{Tor}_{k-1}(F_0,N) = 0$$

Lo stesso discorso funziona anche con $\overline{\operatorname{Tor}}$; l'unica differenza[41] è che questa volta per osservare che $\overline{\operatorname{Tor}}_k(F_0,N)=0$, invece che direttamente la proiettività bisogna usare la piattezza[42]. Dunque $\overline{\operatorname{Tor}}_k(M,N) \cong \overline{\operatorname{Tor}}_{k-1}(\widetilde{M},N)$, e basta ragionare per induzione su k

$$\overline{\operatorname{Tor}}_k(M,N) \cong \overline{\operatorname{Tor}}_{k-1}(\widetilde{M},N) \cong \operatorname{Tor}_{k-1}(\widetilde{M},N) \cong \operatorname{Tor}_k(M,N)$$

che funziona, come già detto, per $k\geq 2$, mentre per $k=1$ basta osservare che $\operatorname{Tor}_1(\widetilde{M},N)$ e $\overline{\operatorname{Tor}}_1(\widetilde{M},N)$ sono isomorfi perché coincidono col Ker della stessa mappa ϵ:

$$\begin{aligned}0 \to \operatorname{Tor}_1(M,N) \to \widetilde{M}\otimes N \xrightarrow{\epsilon} F_0\otimes N \to M\otimes N \to 0 \\ 0 \to \overline{\operatorname{Tor}}_1(M,N) \to \widetilde{M}\otimes N \xrightarrow{\epsilon} F_0\otimes N \to M\otimes N \to 0\end{aligned}$$

□

[41] Questa a prima vista può sembrare una questione di lana caprina, ma prima di gettarla nel dimenticatoio si dia un'occhiata al prossimo Esercizio...

[42] Vedi Osservazione 7.44

Anche questa volta se uno si mette a fare le cose per benino si accorge che l'isomorfismo è naturale in M ed N, cioè che Tor e $\overline{\mathrm{Tor}}$ sono bifuntori naturalmente equivalenti.

Esercizio 7.46. Mostrare che per calcolare $\mathrm{Tor}_k(M, N)$ possiamo utilizzare una risoluzione di M del tipo

$$\cdots \longrightarrow F_4 \longrightarrow F_3 \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$M$$

con gli F_i solo piatti invece che proiettivi.

Hint. Nella dimostrazione del Teorema 7.45 a un certo punto abbiamo enfatizzato che stavamo usando la piattezza e non direttamente la proiettività. Fissando una risoluzione piatta P di M si ottengono gli stessi risultati ottenuti prima per Tor, e invece di $\overline{\mathrm{Tor}}$ si definisce Tor^P come l'omologia di questa risoluzione piatta e le proprietà rilevanti sono abbastanza immediate: ad esempio dove uno scriverebbe $\mathrm{Tor}^P_{k-1}(\widetilde{M}, N) \cong \mathrm{Tor}^P_k(M, N)$ si ritrova a scrivere... $H_k(TP) \cong H_k(TP)$ (shiftando P si ottiene una risoluzione piatta di $\widetilde{M}$...). □

Esercizio 7.47. Se A è un anello commutativo ed M è un A-modulo sono equivalenti

1. M è piatto.
2. Per ogni N si ha $\mathrm{Tor}_1(M, N) = 0$.
3. Come sopra ma per tutti i Tor_k con $k \geq 1$.

Concludiamo il capitolo chiarendo la relazione fra proiettivo, piatto e libero nel caso noetheriano locale. Questo risultato e l'Appendice C sono esempi di come l'algebra omologica "entri" nell'algebra commutativa producendo risultati.

Esercizio 7.48. Siano $(R, \mathfrak{m})$ un anello noetheriano locale, $\mathbb{K} = R/\mathfrak{m}$ il suo campo residuo ed M un R-modulo finitamente generato. Sono equivalenti:

1. M è libero.
2. M è proiettivo.
3. M è piatto.
4. La mappa $\mathfrak{m} \otimes_R M \to R \otimes_R M$ è iniettiva.
5. $\mathrm{Tor}_1(\mathbb{K}, M) = 0$.

Soluzione.

$(1 \Rightarrow 2 \Rightarrow 3)$ È vero in generale e lo sappiamo già[43].

$(3 \Rightarrow 4)$ La successione $0 \to \mathfrak{m} \to R \to \mathbb{K} \to 0$ è esatta. Tensorizzando otteniamo $0 \to \mathfrak{m} \otimes_R M \to R \otimes_R M$ per piattezza di M.

$(4 \Rightarrow 5)$ Partiamo sempre da $0 \to \mathfrak{m} \to R \to \mathbb{K} \to 0$. Per la prima successione esatta lunga di Tor abbiamo

$$\begin{aligned}\operatorname{Tor}_1(R, M) \to \operatorname{Tor}_1(\mathbb{K}, M) \to \operatorname{Tor}_0(\mathfrak{m}, M) \to \\ \to \operatorname{Tor}_0(R, M) \to \operatorname{Tor}_0(\mathbb{K}, M) \to 0\end{aligned}$$

Dato che R è libero $\operatorname{Tor}_1(R, M) = 0$. La successione è quindi

$$0 \to \operatorname{Tor}_1(\mathbb{K}, M) \to \underbrace{\mathfrak{m} \otimes_R M \to R \otimes_R M}_{\text{iniettiva per ipotesi}} \to \mathbb{K} \otimes_R M \to 0$$

e per esattezza $\operatorname{Tor}_1(\mathbb{K}, M)$ non può essere che 0.

$(5 \Rightarrow 1)$ Siano $x_1, \dots, x_n$ elementi di M tali che le loro immagini in $M/\mathfrak{m}M$ siano una sua base come $\mathbb{K}$-spazio vettoriale. Per Nakayama[44] allora $x_1, \dots, x_n$ generano M come R-modulo. Sia F un R-modulo libero generato da $e_1, \dots, e_n$. Definiamo $\varphi\colon F \to M$ come $\varphi(e_i) = x_i$ e mostriamo che è un isomorfismo. La surgettività è ovvia per definizione; posto $E = \operatorname{Ker} \varphi$ consideriamo la successione esatta di R-moduli

$$0 \to E \to F \xrightarrow{\varphi} M \to 0$$

Questa induce la successione esatta lunga di Tor, pensato come funtore derivato sinistro di $\mathbb{K} \otimes_R -$,

$$\cdots \to \operatorname{Tor}_1(\mathbb{K}, M) \to \mathbb{K} \otimes_R E \to \mathbb{K} \otimes_R F \xrightarrow{1 \otimes \varphi} \mathbb{K} \otimes_R M \to 0$$

Dato che $\operatorname{Tor}_1(\mathbb{K}, M) = 0$ per ipotesi, abbiamo

$$0 \to \mathbb{K} \otimes_R E \to \mathbb{K} \otimes_R F \to \mathbb{K} \otimes_R M \to 0$$

I due oggetti a destra sono $\mathbb{K}$-spazi vettoriali, quello centrale di dimensione n, e quello a destra pure, perché è $R/\mathfrak{m} \otimes_R M \cong M/\mathfrak{m}M$. Dunque per esattezza $\mathbb{K} \otimes_R E = 0$. D'altra parte $\mathbb{K} \otimes_R E \cong E/\mathfrak{m}E$, per cui $E = \mathfrak{m}E$ e per Nakayama[45] $E = 0$. Ne segue che $F \cong M$ e M è libero. □

[43] Proposizioni 6.13 e 6.17

[44] Vedi Proposizione 2.8 in [2].

[45] L'ipotesi che R sia noetheriano locale viene usata per poter applicare Nakayama (due volte) nell'ultima implicazione. Nelle altre non è stata usata e quindi restano vere anche rimuovendola.

Capitolo 8

Omologia e Coomologia di Gruppi

8.1 Definizioni

La prima cosa che facciamo è associare ad ogni gruppo G un anello $\mathbb{Z}[G]$. La sua struttura di gruppo abeliano è quella di $\mathbb{Z}$-modulo libero su generatori $g \in G$: un suo elemento è una somma finita $\sum m_g g$, con gli $m_g \in \mathbb{Z}$, e gli elementi si sommano come ci si aspetta. Ci mettiamo sopra una struttura di anello definendo la moltiplicazione sui generatori come[1]

$$1g \cdot 1h \mapsto 1 \cdot (gh)$$

dove a sinistra c'è la moltiplicazione che stiamo definendo su $\mathbb{Z}[G]$ e a destra fra parentesi c'è l'operazione di G. Ad esempio

$$(3g + 2g') \cdot (6h + 2h^{-1}) = 18gh + 6gh^{-1} + 12g'h + 4g'h^{-1}$$

Come esempio concreto, in $\mathbb{Z}[S_3]$, pensando S_3 come funzioni[2]

$$\big(2(12) + 3(132)\big)\big(5(13) + 1 \cdot \mathrm{id}\big) = 10(132) + 2(12) + 15(23) + 3(132)$$

$\mathbb{Z}[G]$ è in generale un anello *non* commutativo; ad esempio $\mathbb{Z}[S_3]$ non lo è.

Se G è un gruppo possiamo definire "G-modulo" un gruppo abeliano A munito di un omomorfismo di gruppi $\Phi\colon G \to \mathrm{Aut}(A)$. Se questo mappa $g \mapsto \varphi_g$, allora la "moltiplicazione per scalare" è

$$g \cdot a = \varphi_g(a) \qquad a \in A$$

[1] D'ora in avanti invece di cose come $1g$ scriveremo direttamente g.

[2] Per capirci: si intende che l'ordine di composizione *non* è come nell'Herstein: in ab agisce prima b e poi a, e $(12)(13) = (132)$.

C'è un'altra maniera di dare ad A una struttura di modulo tramite G: un Φ come sopra si estende a un omomorfismo di anelli[3] $\tilde{\Phi}\colon \mathbb{Z}[G] \to \mathrm{End}(A)$, possiamo dare ad A la struttura di $\mathbb{Z}[G]$-modulo. Questa è moralmente la stessa cosa, ma dato che ora abbiamo fra le mani un modulo "vero" possiamo darlo in pasto all'apparato dei funtori derivati:

Definizione 8.1. Siano G un gruppo e A uno $\mathbb{Z}[G]$-modulo. La *coomologia di G a coefficienti in A* è definita come

$$H^n(G, A) \equiv \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

Ora, A è uno $\mathbb{Z}[G]$-modulo per definizione, ma perché la definizione abbia senso bisogna vedere anche $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo. Ci si mette sopra la struttura banale, in cui ogni $g \in G$ agisce come l'identità, cioè per ogni $n \in \mathbb{Z}$ e $g \in G$ poniamo $g \cdot n = n$ ed estendiamo nella maniera ovvia a tutto $\mathbb{Z}[G]$: per esempio, usando su G la notazione additiva,

$$(g - h) \cdot n = g \cdot n - h \cdot n = n - n = 0$$

In concreto, per calcolare $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ bisogna prendere una risoluzione proiettiva di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo

$$\cdots \longrightarrow P_n \xrightarrow{\delta_n} P_{n-1} \xrightarrow{\delta_{n-1}} \cdots \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$\mathbb{Z}$$

poi si applica[4] $\mathrm{Hom}(-, A)$ ottenendo

$$0 \to \mathrm{Hom}(P_0, A) \xrightarrow{\delta_1^*} \mathrm{Hom}(P_1, A) \xrightarrow{\delta_2^*} \mathrm{Hom}(P_2, A) \xrightarrow{\delta_3^*} \cdots$$

e se ne calcola la coomologia. Ad esempio

$$\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, A) = H^2(P) = \mathrm{Ker}\, \delta_3^* / \mathrm{Im}\, \delta_2^*$$

Ovviamente se ci piace di più possiamo usare una risoluzione iniettiva di A.

Definizione 8.2. Dati un gruppo G e uno $\mathbb{Z}[G]$-modulo destro B, l'*omologia di G a coefficienti in B* è

$$H_n(G, B) = \mathrm{Tor}^{\mathbb{Z}[G]}_n(B, \mathbb{Z})$$

Anche qui $\mathbb{Z}$ si intende munito della struttura di $\mathbb{Z}[G]$-modulo banale.

[3] In arrivo non c'è più $\mathrm{Aut}(A)$ ma $\mathrm{End}(A)$ perché in $\mathbb{Z}[G]$ abbiamo la somma e quindi l'endomorfismo nullo, e probabilmente un sacco di altri endomorfismi non invertibili. Si pensi al caso in cui G è un gruppo di matrici e la somma di $\mathbb{Z}[G]$ è l'usuale somma di matrici...

[4] Qui chiaramente gli omomorfismi sono tutti di $\mathbb{Z}[G]$-moduli, ma ho evitato di scrivere $\mathrm{Hom}_{\mathbb{Z}[G]}$ ovunque.

8.2 H^0 e H_0

$H^0(G, A)$ è per definizione $\operatorname{Ker} \delta_1^*$. Dato[5] che $\operatorname{Hom}(-, A)$ è esatto a sinistra prendendo una sua risoluzione proiettiva, completandola a successione esatta[6] e applicando $\operatorname{Hom}(-, A)$ abbiamo

$$0 \to \operatorname{Hom}(\mathbb{Z}, A) \to \operatorname{Hom}(P_0, A) \xrightarrow{\delta_1^*} \operatorname{Hom}(P_1, A) \xrightarrow{\delta_2^*} \operatorname{Hom}(P_2, A) \xrightarrow{\delta_3^*} \cdots$$

e $H^0(G, A) \simeq \operatorname{Hom}(\mathbb{Z}, A)$.

Com'è fatto un elemento di $\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$? Come tutti i bravi omomorfismi di gruppi abeliani che partono da $\mathbb{Z}$ è determinato da $\varphi(1) = a$. Inoltre per essere un omomorfismo di $\mathbb{Z}[G]$-moduli deve soddisfare $\varphi(\lambda x) = \lambda\varphi(x)$, e in particolare $\varphi(g \cdot 1) = g \cdot \varphi(1)$. Dato che la struttura di $\mathbb{Z}[G]$-modulo su $\mathbb{Z}$ è quella banale abbiamo $\varphi(g \cdot 1) = \varphi(1)$. Ma allora

$$a = \varphi(1) = \varphi(g \cdot 1) = g\varphi(1) = g \cdot a$$

In altre parole a è invariante per G, per cui[7] $\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G$ è il *sottomodulo degli invarianti*, cioè

$$\{x \in A \mid \forall g \in G\ gx = x\}$$

Già l'H^0 quindi contiene un bel po' di informazione. Chi è invece l'H_0? Per scoprirlo bisogna fare la conoscenza di un altro signore, che comunque tornerà in gioco quando parleremo dell'H^1:

Definizione 8.3. La mappa di *augmentazione* è l'omomorfismo di anelli $\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ definito come $\epsilon\left(\sum m_g g\right) = \sum m_g$ oppure, equivalentemente, $\forall g \in G\ \epsilon(g) = 1$. Chiamiamo $IG = \operatorname{Ker} \epsilon$ l'*ideale di augmentazione*.

Denotando[8] con e l'identità di G, dato che l'azione di G è quella banale, per ogni $g \in G$ si ha $g - e \in IG$. Non solo:

Proposizione 8.4. IG è lo $\mathbb{Z}$-modulo libero generato dai $g - e$ al variare di g in $G \setminus \{e\}$.

Dimostrazione. Chiaramente vale[9] $\langle g-e\rangle_{g\in G,\mathbb{Z}} \subseteq IG$. Viceversa se $\sum m_g g \in \operatorname{Ker} \epsilon$ per definizione vale $\sum m_g = 0$; ma allora basta scrivere

$$\sum m_g g = \sum m_g g - \underbrace{\left(\sum m_g\right)}_{=0} e = \sum m_g (g - e)$$

[5] Questo discorso l'abbiamo già fatto, ma per comodità psicologica lo ripetiamo.

[6] Nel senso che stiamo inserendo $\mathbb{Z}$ fra P_0 e 0.

[7] Abbiamo mostrato una condizione necessaria su $\varphi(1) = a$, ma è palese che sia anche sufficiente, cioè che per ogni a che verifica quanto sopra si può definire φ tale che $\varphi(1) = a$.

[8] A un certo punto inizieremo anche a denotarla con 1; in letteratura sono comuni entrambi gli usi.

[9] Quello $\mathbb{Z}$ indica che è lo span su $\mathbb{Z}$.

Quanto al "libero", se $\sum m_g(g-e)=0$ allora

$$\sum m_g g = \sum m_g e = \left(\sum m_g\right) e = 0$$

ma i g sono $\mathbb{Z}$-indipendenti per definizione di $\mathbb{Z}[G]$, e quindi $\forall g\ m_g = 0$. □

Dunque conosciamo abbastanza bene la struttura di $\mathbb{Z}$-modulo di IG. Che dire della sua struttura di $\mathbb{Z}[G]$-modulo?

Proposizione 8.5. IG è generato come $\mathbb{Z}[G]$-modulo dagli $x-e$ al variare di x in un insieme di generatori di G.

Dimostrazione. Per la Proposizione precedente ci basta mostrare che, se $z-e$ e $y-e$ sono combinazione $\mathbb{Z}[G]$-lineare degli $x-e$, allora anche $zy-e$ e $z^{-1}-e$ lo sono. Questo è vero perché possiamo scrivere

$$zy-e = z(y-e)+(z-e) \qquad z^{-1}-e = -z^{-1}(z-e)$$ □

Siamo pronti per calcolare $H_0(G,B)$, che per definizione è $\operatorname{Tor}_0^{\mathbb{Z}[G]}(B,\mathbb{Z})$, dove $\mathbb{Z}$ è munito della struttura di $\mathbb{Z}[G]$-modulo banale. Prendiamo al solito una risoluzione proiettiva

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$\mathbb{Z}$$

e tensorizziamo ottenendo

$$\cdots \to B \otimes_{\mathbb{Z}[G]} P_2 \to B \otimes_{\mathbb{Z}[G]} P_1 \to B \otimes_{\mathbb{Z}[G]} P_0 \to 0$$

La situazione qui è analoga a quella dell'H^0: vista l'esattezza a destra di $B \otimes_{\mathbb{Z}[G]} -$, prolungando la risoluzione a successione esatta e tensorizzando troviamo $B \otimes_{\mathbb{Z}[G]} P_1 \to B \otimes_{\mathbb{Z}[G]} P_0 \to B \otimes_{\mathbb{Z}[G]} \mathbb{Z} \to 0$ e quindi $H_0(G,B) = B \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Dati un suo generatore $b \otimes_{\mathbb{Z}[G]} n$ e un qualunque $g \in G$ abbiamo[10]

$$bg \otimes_{\mathbb{Z}[G]} n = b \otimes_{\mathbb{Z}[G]} gn = b \otimes_{\mathbb{Z}[G]} n$$

Dunque possiamo scrivere l'isomorfismo di gruppi abeliani[11]

$$B \otimes_{\mathbb{Z}[G]} \mathbb{Z} \cong \frac{B \otimes_{\mathbb{Z}} \mathbb{Z}}{\langle bg \otimes_{\mathbb{Z}} 1 - b \otimes_{\mathbb{Z}} 1\rangle}$$

Passando per l'isomorfismo $B \otimes_{\mathbb{Z}} \mathbb{Z} \cong B$ in definitiva abbiamo

$$H_0(G,B) \cong \frac{B}{\langle bg-b\rangle} = \frac{B}{\langle b(g-e)\rangle} = \frac{B}{B\cdot IG}$$

[10] Si noti la posizione di g: avevamo detto che l'elemento a sinistra del tensore deve essere un modulo destro e quello a destra un modulo sinistro...

[11] Occhio all'anello su cui si tensorizza!!

Dalla riga sopra è chiaro che se G agisce su B banalmente allora $H_0(G, B) = B$, perché in tal caso $b(x - e) = b - b = 0$. Se l'azione non è banale comunque "la ritroviamo" nell'H_0, nel senso che i generatori del modulo per cui quozientiamo misurano in un certo senso la "distanza" fra b e le sue immagini secondo l'azione.

8.3 Un Po' di Fumo

Segue una digressione/raccontino sul collegamento con la geometria.

Nei primi anni '30 i topologi (Hurewicz, tipo) si resero conto che se (X, x_0) è uno spazio topologico puntato connesso, localmente semplicemente connesso e tale che il suo rivestimento universale $\tilde{X}$ è n-connesso[12], allora i suoi gruppi di omologia dipendevano solo dal π_1. Dunque l'omologia $H_n(X, \mathbb{Z})$ "doveva" in un qualche modo esprimersi in termini puramente algebrici di $\pi_1(X)$. La cosa fu sistemata da Hopf:

Teorema 8.6 (Hopf)**.** Sotto le ipotesi di cui sopra per $1 \leq i \leq n$ si ha $H_i(X, \mathbb{Z}) \cong H_i(\pi_1(X), \mathbb{Z})$, dove $\mathbb{Z}$ è visto come $\pi_1(X)$-modulo in modo banale. Dunque $H_i(\pi_1(X), \mathbb{Z})$ è $\operatorname{Tor}_i^{\mathbb{Z}[\pi_1(X)]}(\mathbb{Z}, \mathbb{Z})$.

Ma allora l'omologia degli spazi poteva essere calcolata calcolando l'omologia dei gruppi, e la cosa è andata avanti rimbalzando fra topologi e algebristi.

La cosa funziona anche nell'altro verso: uno spazio $K(G, 1)$ è uno spazio tale che $\pi_1(X) = G$ e tutti π_n per $n \geq 2$ sono banali, e dato un qualunque gruppo G si può costruire un CW-complesso $K(G, 1)$. Gli spazi $K(G, 1)$ hanno rivestimento universale $\tilde{X}$ tale che $\pi_n(\tilde{X}) = 0$, e quindi siamo nelle ipotesi del Teorema di Hopf. Dunque se vogliamo calcolare l'omologia di G a coefficienti in $\mathbb{Z}$ possiamo costruirci un X spazio $K(G, 1)$ e sperare di saper calcolare la sua omologia a coefficienti in $\mathbb{Z}$.

A che serve aver fatto tutta le teoria con moduli qualunque se esce fuori sempre $\mathbb{Z}$ con la struttura banale? È collegato all'omologia di certi spazi che saltano fuori come fibrazioni.

8.4 Il Primo Gruppo di Coomologia

Scopo di questa sezione è mostrare che $H^1(G, A)$ consiste delle "derivazioni del gruppo modulo le derivazioni interne". Che vuol dire?

[12] Vuol dire che $\pi_1(X) = \pi_2(X) = \ldots = \pi_n(X) = \{e\}$, dove π_k è il k-esimo gruppo di omotopia.

Definizione 8.7. Siano G un gruppo e A uno $\mathbb{Z}[G]$-modulo. Una *derivazione*[13] è una funzione $\varphi\colon G \to A$ tale che[14] $\varphi(xy) = \varphi(x) + x\varphi(y)$. L'insieme delle derivazioni $\mathrm{Der}(G, A)$ è un gruppo abeliano (con la somma).

Osservazione 8.8. Se φ è una derivazione $\varphi(e) = 0$, perché $\varphi(e) = \varphi(e^2) = \varphi(e) + e\varphi(e)$. Dunque $\varphi(e) = 2\varphi(e)$, per cui $\varphi(e) = 0$.

Teorema 8.9. Il funtore $\mathrm{Der}(G, -)\colon \mathscr{M}^{\ell}_{\mathbb{Z}[G]} \to \mathrm{Ab}$ è *rappresentato* da IG, ovvero esiste η equivalenza naturale fra $\mathrm{Der}(G, -)$ e $\mathrm{Hom}_{\mathbb{Z}[G]}(IG, -)$.

Dimostrazione. Fissato uno $\mathbb{Z}[G]$-modulo A definiamo $\eta_A\colon \mathrm{Der}(G, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(IG, A)$ nella seguente maniera: forti delle Proposizioni 8.4 e 8.5, se d è una derivazione definiamo $\eta_A(d)\colon IG \to A$ come

$$\eta_A(d)(y - e) = d(y)$$

Questo intanto è un omomorfismo di gruppi abeliani, ed è ben definito perché per la Proposizione 8.4 IG è uno $\mathbb{Z}$-modulo libero. Per verificare che $\eta_A(d)$ è effettivamente un omomorfismo di $\mathbb{Z}[G]$-moduli bisogna vedere che

$$\eta_A(d)(g \cdot (y - e)) \stackrel{?}{=} g \cdot \eta_A(d)(y - e)$$

partiamo da sinistra:

$$\begin{aligned}\eta_A(d)(g(y - e)) &= \eta_A(d)((gy - e) - (g - e)) \\ &= \eta_A(d)(gy - e) - \eta_A(d)(g - e) = \underbrace{d(gy) - d(g) = gd(y)}_{\text{definizione di derivazione}} = g\eta_A(d)(y - e)\end{aligned}$$

La mappa inversa $\eta_A^{-1} = \xi_A\colon \mathrm{Hom}_{\mathbb{Z}[G]}(IG, A) \to \mathrm{Der}(G, A)$ è definita come

$$\xi_A(\varphi)(y) = \varphi(y - e)$$

Verifichiamo che $\xi_A(\varphi)$ è una derivazione:

$$\begin{aligned}\xi_A(\varphi)(xy) = \varphi(xy - e) &= \varphi(x(y - e) + (x - e)) \\ &= x\varphi(y - e) + \varphi(x - e) = x\xi_A(\varphi)(y) + \xi_A(\varphi)(x)\end{aligned}$$

La verifica che le mappe sono una l'inversa dell'altra e che sono trasformazioni naturali è lasciata al lettore[15]. □

C'è ancora da dire cosa vuol dire che una derivazione è *interna*:

[13] In inglese *derivation*, ma anche *crossed homomorphism*.
[14] No, non è un errore di stampa. Vicino a $\varphi(x)$ non c'è nessun y.
[15] Ma il lettore pigro può trovarla in [4], Teorema 70, pagina 96.

Definizione 8.10. $\mathrm{IDer}(G, A)$ è il sottogruppo di $\mathrm{Der}(G, A)$ dato dalle *derivazioni interne*[16] d_a (al variare di $a \in A$) definite come

$$d_a(x) = (x - e)a$$

Questa d_a è una derivazione? Sì, col solito trucco:

$$d_a(xy) = (xy - e)a = [x(y - e) + (x - e)]a = xd_a(y) + d_a(x)$$

Come ci si aspetta, $d_a + d_b = d_{a+b}$, e quindi IDer è effettivamente un sottogruppo di Der.

Siamo finalmente pronti per calcolare $H^1(G, A) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Invece che una risoluzione, scegliamo una presentazione[17] proiettiva di $\mathbb{Z}$ (come $\mathbb{Z}[G]$-modulo, ovviamente). Una "ce la siamo già detta" ed è l'augmentazione[18]:

$$0 \to IG \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

che è una presentazione proiettiva perché $\mathbb{Z}[G]$, in quanto banalmente libero, è proiettivo. Applicando $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A)$ otteniamo la successione esatta

$$0 \to \mathrm{Hom}(\mathbb{Z}, A) \to \mathrm{Hom}(\mathbb{Z}[G], A) \xrightarrow{i^*} \mathrm{Hom}(IG, A)$$

Combinando quanto visto con la Proposizione 7.23 abbiamo quindi

$$\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong \mathrm{Coker}\, i^* = \frac{\mathrm{Hom}(IG, A)}{i^*(\mathrm{Hom}(\mathbb{Z}[G], A))} \overset{\xi_A}{\cong} \frac{\mathrm{Der}(G, A)}{\textcircled{?}}$$

e per completare il quadro bisogna capire chi è $\textcircled{?}$. Per definizione $\mathrm{Im}\, i^*$ consiste delle mappe $\psi \circ i$, al variare di $\psi \in \mathrm{Hom}(\mathbb{Z}[G], A)$, dunque dobbiamo vedere chi è $\xi_A(\psi \circ i)$. Per definizione

$$\xi_A(\psi \circ i)(x) = \psi \circ i(x - e) = \psi(x - e)$$

e dato che $\mathbb{Z}[G]$ è libero ψ è deciso da $\psi(e) = a$, per cui

$$\psi(x - e) = \psi((x - e)e) = (x - e)\psi(e) = (x - e)a = d_a(x)$$

e quindi come promesso $\textcircled{?} = \langle d_a \mid a \in A \rangle = \mathrm{IDer}(G, A)$ e l'H^1 è "derivazioni modulo derivazioni interne". Vediamo qualche esempio concreto.

Esempio 8.11. Sia $C_m = \langle x \rangle$ il gruppo ciclico di ordine m e sia $A = (\mathbb{Z}/2\mathbb{Z})^m$, dove la struttura di $\mathbb{Z}[C_m]$ modulo è data dichiarando che il generatore x agisce come

$$x(a_1, \ldots, a_m) = (a_m, a_1, \ldots, a_{m-1})$$

[16] In inglese *inner derivations* o *principal crossed homomorphisms*.

[17] Anche perché (per ora) non abbiamo risoluzioni fra le mani.

[18] Occhio: IG è libero come $\mathbb{Z}$-modulo, non come $\mathbb{Z}[G]$-modulo, quindi questa *non* è (in generale) una risoluzione, ma solo una presentazione.

Per capire chi è $H^1(C_m, (\mathbb{Z}/2\mathbb{Z})^m)$ passiamo per le derivazioni, per cui iniziamo a cercare di capire com'è fatto $\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m)$. Per l'Osservazione 8.8 $d(e) = 0$. Se $d(x) = (a_1, \ldots, a_m)$, allora $d(x^2) = xd(x) + d(x)$, e similmente $d(x^3) = x^2 d(x) + xd(x) + d(x)$ eccetera. Quando arriviamo ad m abbiamo

$$0 = d(e) = d(x^m) = x^{m-1}d(x) + \ldots + xd(x) + d(x)$$

Per com'è fatta l'azione di x questo vuol dire che

$$\begin{aligned} 0 = (a_1, \ldots\ldots\ldots, a_m) + \\ (a_m, \ldots\ldots, a_{m-1}) + \\ (a_{m-1}, \ \ldots, \ a_{m-2}) + \\ \vdots \quad \vdots \quad \vdots \quad \vdots \end{aligned}$$

Le derivazioni mappano quindi[19] $d(x) = (a_1, \ldots, a_m)$ con $\sum a_i = 0$, e possiamo scrivere

$$\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m) \cong \mathrm{Ker}(e + x + x^2 + \ldots + x^{m-1})$$

dove stiamo identificando una derivazione d con l'immagine $d(x)$ del generatore di C_m, e con $\mathrm{Ker} \sum x^i$ si intende il nucleo della mappa $\mathbb{Z}[C_m]$-lineare[20] $A \to A$ data dalla moltiplicazione per $\sum x^i \in \mathbb{Z}[C_m]$. Chi sono le derivazioni interne? Se $b \in (\mathbb{Z}/2\mathbb{Z})^m$, allora per definizione $d_b(x) = (x - e)b$, per cui, con la stessa identificazione di poco fa,

$$\mathrm{IDer} \cong \mathrm{Im}(x - e)$$

Ne segue che

$$\frac{\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m)}{\mathrm{IDer}(C_m, (\mathbb{Z}/2\mathbb{Z})^m)} \cong \frac{\mathrm{Ker}(e + x + \ldots + x^{m-1})}{\mathrm{Im}(x - e)}$$

Le mappe $\sum x^i$ ed $x - e$, oltre ad essere mappe $\mathbb{Z}[C_m]$-lineari, sono mappe lineari fra $(\mathbb{Z}/2\mathbb{Z})$-spazi vettoriali $(\mathbb{Z}/2\mathbb{Z})^m \to (\mathbb{Z}/2\mathbb{Z})^m$. La mappa $x - e$, nella base standard, ha come matrice

$$\begin{pmatrix} -1 & 0 & \ldots & 0 & 1 \\ 1 & -1 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & -1 & 0 \\ 0 & 0 & \ldots & 1 & -1 \end{pmatrix}$$

[19] Anche qui abbiamo mostrato solo la necessità, ma la sufficienza è immediata.
[20] Cioè omomorfismo di $\mathbb{Z}[C_m]$-moduli.

che si vede facilmente[21] avere rango $m-1$. D'altra parte $\dim \mathrm{Ker}(e+x+\ldots+x^{m-1}) \leq m-1$, perché $(1,0,\ldots,0)$ viene mappato in $(1,1,\ldots,1) \neq 0$. Ne segue che $H^1(C_m, (\mathbb{Z}/2\mathbb{Z})^m) = 0$.

Esempio 8.12. Prendiamo $C_2 = \{e, x\}$ e facciamolo agire su $\mathbb{Z}$ nell'unica maniera non banale, cioè $xn = -n$.

Chi è $\mathrm{Der}(C_2, \mathbb{Z})$? Se $d(x) = m$, allora $d(x^2) = xd(x) + d(x) = 0$. Quindi in ogni caso $d(x^2) = d(e)$ e qualunque scelta di $m \in \mathbb{Z}$ va bene, per cui $\mathrm{Der}(C_2, \mathbb{Z}) \cong \mathbb{Z}$. Guardiamo ora $\mathrm{IDer}(C_2, \mathbb{Z})$: identificando anche qui una derivazione interna d_n col suo valore in x, abbiamo

$$d_n(x) = (x-e)n = xn - en = -n - n = -2n$$

Dunque $\mathrm{IDer}(C_2, \mathbb{Z}) \cong 2\mathbb{Z}$ e in definitiva $H^1(C_2, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

8.5 Alla Ricerca di Risoluzioni Proiettive

Visto che vorremmo calcolare anche gli H^n ed H_n con $n \geq 2$, presentiamo una risoluzione proiettiva comoda di $\mathbb{Z}$ visto come C_m-modulo banale. Questa è

$$\cdots \longrightarrow \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{T} \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{T} \mathbb{Z}[C_m] \longrightarrow 0$$
$$\mathbb{Z}[C_m] \searrow^{\epsilon} \quad \nearrow \mathbb{Z}$$

dove $T(e) = x - e$ e $N(e) = e + x + \ldots + x^{m-1}$. È facile vedere $N \circ T$ e $T \circ N$ sono nulle, per cui quello che abbiamo disegnato sopra è un complesso, e dato che $\mathrm{Im}\, T = IG$ effettivamente[22] l'H_0 del complesso è $\mathbb{Z}$. Dato che $\mathbb{Z}[C_m]$ è proiettivo in quanto libero, per affermare di aver esibito una risoluzione proiettiva ci resta da mostrarne l'aciclicità.

Dato $y \in \mathrm{Ker}\, T$, scrivendolo come $y = \sum a_h x^h$, cioè come combinazione dei generatori di $\mathbb{Z}[C_m]$ come $\mathbb{Z}$-modulo, abbiamo

$$0 = T(y) = \Big(\sum_{h=0}^{m-1} a_h x^h\Big)(x-1)$$

Perché il membro a destra sia nullo deve esserlo ogni sua coordinata negli x^h, e per com'è fatta la somma (è telescopica) deve valere $a_0 = a_1 = \ldots = a_m = \tilde{a}$. Allora $y = (1 + x + \ldots + x^{m-1})\tilde{a}$ e $y \in \mathrm{Im}\, N$. L'altra inclusione ce l'avevamo già e quindi $\mathrm{Ker}\, T = \mathrm{Im}\, N$. La verifica che $\mathrm{Ker}\, N \subseteq \mathrm{Im}\, T$ è lasciata al lettore[23].

[21] La somma delle colonne è nulla e tutti i minori di testa "veri" (non tutta la matrice) sono già in forma di Jordan...

[22] In caso non fosse chiaro: ϵ è l'augmentazione.

[23] In [4] è all'interno dell'Esercizio 20, pagina 98.

Veniamo all'omologia. Ricordiamo che $H_m(C_m, \mathbb{Z}) = \mathrm{Tor}_n^{\mathbb{Z}[C_m]}(\mathbb{Z}, \mathbb{Z})$. Tensorizzando la risoluzione appena presentata otteniamo

$$\cdots \xrightarrow{T\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \xrightarrow{N\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \xrightarrow{T\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \to 0$$

usando i soliti isomorfismi questa sarebbe $\cdots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to 0$, ma chi sono le mappe? Dato che $T(1) = x - 1$ e che $\mathbb{Z}$ ha la struttura di $\mathbb{Z}[C_m]$ modulo banale, $(x-1)n$ è sempre 0, per cui una mappa l'abbiamo identificata; per lo stesso motivo è immediato accorgersi che la mappa indotta da N è la moltiplicazione per m, per cui in definitiva abbiamo

$$\cdots \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0$$

e possiamo finalmente calcolare l'omologia:

- $H_0(C_m, \mathbb{Z}) = \mathbb{Z}$
- $H_{2k+1}(C_m, \mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$
- $H_{2k+2}(C_m, \mathbb{Z}) = 0$.

Dunque tutti i gruppi di omologia dispari sono non nulli. Questo ha come conseguenza immediata il fatto che

Corollario 8.13. $\mathbb{Z}$ non ha risoluzioni proiettive finite (ossia definitivamente nulle) come $\mathbb{Z}[C_m]$-modulo.

Dimostrazione. Se ce ne fosse una i gruppi di omologia sarebbero definitivamente nulli. □

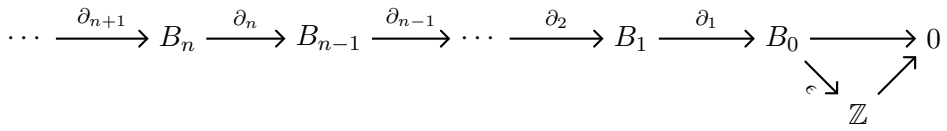
Se ci si mette a calcolare la coomologia[24] viene fuori che la situazione è analoga ma a ruoli invertiti:

- $H^0(C_m, \mathbb{Z}) = \mathbb{Z}$
- $H^{2k+1}(C_m, \mathbb{Z}) = 0$
- $H^{2k+2}(C_m, \mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$.

Gli appassionati di Teoria di Galois possono trovare un'applicazione di quanto fatto finora in [4], a pagina 99.

Nell'esempio visto poco fa siamo "stati fortunati" e abbiamo trovato una risoluzione proiettiva di $\mathbb{Z}$ come $\mathbb{Z}[C_m]$-modulo banale particolarmente comoda. Cosa fare se invece di C_m c'è un qualunque gruppo G? In mancanza di idee furbe, ci sono comunque alcune risoluzioni proiettive di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo banale che, sebbene molto grandi, sono disponibili sempre. Una si chiama *bar-resolution omogenea*, e la presentiamo così:

[24] Basta usare la stessa risoluzione



dove B_n è lo $\mathbb{Z}[G]$-modulo definito nella seguente maniera: si parte dallo $\mathbb{Z}$-modulo generato da tutte le $n+1$-uple $(y_0, \dots, y_n) \in G^{n+1}$ e si definisce l'azione di G ponendo, per $y \in G$,

$$y(y_0, \dots, y_n) = (yy_0, \dots, yy_n)$$

B_n è uno $\mathbb{Z}[G]$-modulo proiettivo, anzi è addirittura libero[25], e una sua base è $\{(1, y_1, \dots, y_n) \mid y_i \in G\}$. Chi sono le mappe? ϵ è l'augmentazione[26], mentre il differenziale $\partial_n \colon B_n \to B_{n-1}$ è definito come

$$\partial_n(y_0, \dots, y_n) = \sum_{i=0}^{n} (-1)^i (y_0, \dots, \hat{y_i}, \dots, y_n)$$

dove il cappuccio indica la coordinata rimossa. Questo compare anche in altre costruzioni in topologia, e ogni volta che si definisce una mappa del genere vale $\partial_{n-1} \circ \partial_n = 0$, per cui assumiamo che il lettore abbia già fatto questa verifica una volta nella vita[27]. La parte ingegnosa è mostrare che

Esercizio 8.14. Questa è effettivamente una risoluzione.

Soluzione. Allunghiamo[28] il complesso definendo $B_{-1} = \mathbb{Z}$ e $\partial_0 = \epsilon$:

$$\cdots \xrightarrow{\partial_{n+1}} B_n \xrightarrow{\partial_n} B_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

Se lo guardiamo come complesso di $\mathbb{Z}$-moduli, cioè di gruppi abeliani, e mostriamo che ha omologia nulla abbiamo simultaneamente l'aciclicità del complesso di partenza B e il fatto che $H_0(B) \cong \mathbb{Z}$. A tale scopo è sufficiente mostrare che l'identità e la mappa nulla sono omotope[29], cioè trovare Σ tale che[30] $\partial \circ \Sigma + \Sigma \circ \partial = \mathrm{id} - 0$:

[25] Verifiche su [4] a pagina 101.

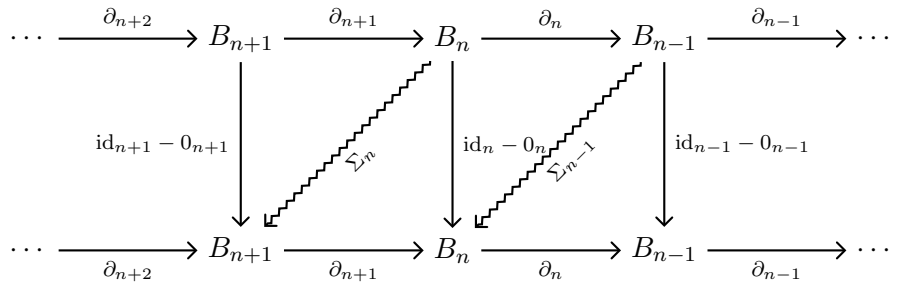
[26] Ha senso: $B_0 \cong G$.

[27] Il trucco è che in $\partial_n(\partial_{n-1}(y_0, \dots, y_n))$ ci saranno due termini "senza y_i e y_j", ma dato che in uno è scomparso prima y_i e in uno prima y_j...

[28] A volte questo viene chiamato *complesso augmentato*.

[29] Vedi Osservazione 7.9.

[30] Chiaramente il -0 ce lo possiamo dimenticare: è lì per comodità psicologica.

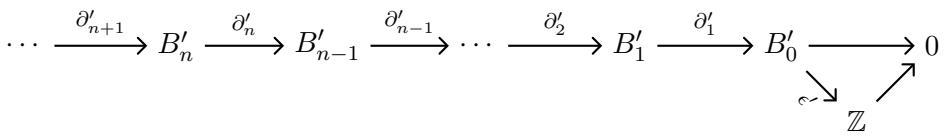


Una Σ che funziona[31] è

$$\begin{cases} \Sigma_{-1}(1) = 1 \\ \Sigma_n((y_0, \ldots, y_n)) = (1, y_0, \ldots, y_n) \quad \text{se } n \geq 0 \end{cases}$$

□

Il difetto della bar-resolution omogenea è che tende ad essere parecchio grande. Un'altra risoluzione standard è la *bar-resolution non omogenea*



dove per n positivo B'_n è lo $\mathbb{Z}[G]$-modulo libero sulle n-uple di elementi di G denotate come

$$[x_1 \mid x_2 \mid \ldots \mid x_n]$$

mentre B'_0 è lo $\mathbb{Z}[G]$-modulo libero con base $\{[\,]\}$ e $\epsilon'([\,]) = 1$. Dato che su $\mathbb{Z}$ stiamo considerando la struttura di $\mathbb{Z}[G]$-modulo banale, si ha anche

$$\epsilon'(g[\,]) = g\epsilon'([\,]) = g \cdot 1 = 1$$

Le mappe di bordo sono fatte in questa maniera:

$$\begin{aligned} \partial'_n([x_1 \mid x_2 \mid \ldots \mid x_n]) &= x_1[x_2 \mid \ldots \mid x_n] + \\ &+ \Big(\sum_{i=1}^{n-1} (-1)^i [x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n]\Big) + (-1)^n [x_1 \mid \ldots \mid x_{n-1}] \end{aligned}$$

Fra i due complessi $\{B_j\}$ e $\{B'_j\}$ c'è un isomorfismo $\varphi\colon B \to B'$ dato dalle

$$\varphi_n(1, y_1, \ldots, y_n) = [y_1 \mid y_1^{-1}y_2 \mid y_2^{-1}y_3 \mid \ldots \mid y_{n-1}^{-1}y_n]$$

Perché i quadrati[32] commutano? Ad esempio

$$\begin{aligned} &(1, y_1, y_2) \xrightarrow{\varphi_2} [y_1 \mid y_1^{-1}y_2] \xrightarrow{\partial'_2} y_1[y_1^{-1}y_2] - [y_1 y_1^{-1} y_2] + [y_1] \\ &= y_1[y_1^{-1}y_2] - [y_2] + [y_1] \end{aligned}$$

[31] Per le verifiche vedi [4], pagina 102.

[32] Dovrebbe essere chiaro di quale diagramma: cos'è un morfismo di complessi?

mentre

$$(1, y_1, y_2) \xrightarrow{\partial_2} (y_1, y_2) - (1, y_2) + (1, y_1) \xrightarrow{\varphi_1} ?$$

e vediamo subito che

$$\varphi_1(y_1, y_2) = \varphi_1(y_1(1, y_1^{-1}y_2)) = y_1\varphi_1((1, y_1^{-1}y_2)) = y_1[y_1^{-1}y_2]$$

Altrettanto facilmente si vede $\varphi_1((1, y_2)) = [y_2]$ e $\varphi_1((1, y_1)) = [y_1]$. Analogamente anche gli altri quadrati commutano, e quindi φ è effettivamente un morfismo di complessi. L'inversa di φ è $\psi\colon B' \to B$ data dalle

$$\psi_n([x_1 \mid \ldots \mid x_n]) = (1, x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2\cdots x_n)$$

Questo mostra che la bar resolution non omogenea è una risoluzione proiettiva, perché isomorfa a quella omogenea, che abbiamo già visto esserlo. Altrimenti si può considerare direttamente l'omotopia[33]

$$\begin{cases} \bar{\Delta}_{-1}(1) = [\,] \\ \bar{\Delta}_n(x[x_1 \mid \ldots \mid x_n]) = [x \mid x_1 \mid \ldots \mid x_n] \quad \text{se } n \geq 0 \end{cases}$$

8.6 Il Secondo Gruppo di Coomologia

Se non abbiamo idee geniali come nel caso di C_m, la bar resolution non omogenea ci permette di calcolare comunque l'H^2.

Esercizio 8.15 (Illuminante)**.** Dati G e A individuare i 2-cocicli, ossia $\operatorname{Ker}\partial_3^*$, all'interno del complesso

$$0 \to \operatorname{Hom}(B_0', A) \xrightarrow{\partial_1^*} \operatorname{Hom}(B_1', A) \xrightarrow{\partial_2^*} \operatorname{Hom}(B_2', A) \xrightarrow{\partial_3^*} \operatorname{Hom}(B_3', A) \xrightarrow{\partial_4^*} \cdots$$

Soluzione. Una $f \in \operatorname{Hom}_{\mathbb{Z}[G]}(B_2', A)$ è decisa dai valori $f([x \mid y])$. Dunque associamo ad f una funzione[34], che chiamiamo ancora f, da $G \times G$ in A, definita come

$$f\colon G \times G \to A \qquad f(x, y) = f([x \mid y])$$

Vediamo chi è $\operatorname{Ker}\partial_3^*$. Se f ci appartiene vuol dire che $\partial_3^* f = 0$ e quindi, ricordandoci chi è il differenziale della bar resolution non omogenea, abbiamo

$$\begin{aligned} 0 &= \partial_3^* f([x \mid y \mid z]) \\ &= f \circ \partial_3([x \mid y \mid z]) \\ &= f\big(x[y \mid z] + (-[xy \mid z] + [x \mid yz]) - [x \mid y]\big) \\ &= xf([y \mid z]) - f([xy \mid z]) + f([x \mid yz]) - f([x \mid y]) \end{aligned}$$

Dunque f, vista come mappa $G \times G \to A$, è un 2-cociclo se e solo se soddisfa la relazione sopra, che riscriviamo come

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0 \qquad \square$$

[33] Sì, è $\varphi \circ \Sigma \circ \psi$.

[34] E basta; non è un omomorfismo né niente più che una funzione.

Più in generale possiamo associare ad un complesso i morfismi nella categoria degli insiemi come con le parentesi graffe qui:

$$0 \to \underbrace{\mathrm{Hom}_{\mathbb{Z}[G]}(B'_0, A)}_{F\colon \{*\}\to A} \to \underbrace{\mathrm{Hom}_{\mathbb{Z}[G]}(B'_1, A)}_{F\colon G\to A} \to \underbrace{\mathrm{Hom}_{\mathbb{Z}[G]}(B'_2, A)}_{F\colon G\times G\to A} \to \cdots$$

e come visto qui sopra il differenziale si "traduce" a livello insiemistico, dove ∂_n^* si legge come

$$\begin{aligned}\partial_n^* f(x_1, \ldots, x_{n+1}) &= x_1 f(x_2, \ldots, x_{n+1}) + \\ &+ \sum_{i=1}^{n-1} (-1)^i f(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^n f(x_1, \ldots, x_n)\end{aligned}$$

Questa è un'altra maniera di presentare la coomologia di gruppi $H^n(G, A)$, dando funzioni e questo "strano" differenziale. Il vantaggio che abbiamo noi è che sappiamo che questa è quella che viene dalla bar resolution non omogenea, ma che comunque possiamo usare anche altre risoluzioni, qualora dovessero semplificare il lavoro.

Ora capiamo finalmente cosa rappresenta/calcola $H^2(G, A)$. Se G un gruppo e A un G-modulo possiamo parlare del prodotto semidiretto $A \rtimes G$: infatti A in quanto modulo possiede una struttura di gruppo abeliano, e per definizione di G-modulo abbiamo un morfismo $G \to \mathrm{Aut}(A)$ che mappa g in $a \mapsto ga$, e in $H \rtimes K$ il prodotto era $(h, k)(h_1, k_1) = (h\vartheta(k)(h_1), kk_1)$, dove $K \xrightarrow{\vartheta} \mathrm{Aut}\, H$ è fissato. Nel nostro caso ϑ è quello dato dalla struttura di G-modulo, e abbiamo

$$\begin{gathered}A \rtimes G = \{(a, g) \mid a \in G, g \in G\} \\ (a, g)(a_1, g_1) = (a + g \cdot a_1, gg_1) \\ (a, g)^{-1} = (-g^{-1}a, g^{-1})\end{gathered}$$

Abbiamo la successione esatta di gruppi[35]

$$1 \to A \xrightarrow{i} A \rtimes G \xrightarrow{\pi} G \to 1$$

Consideriamo adesso G, un G-modulo A e una successione esatta di gruppi

$$1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

Qui A è abeliano e, dato che $i(A) = \mathrm{Ker}\, p$ per esattezza, $i(A)$ è un sottogruppo normale di E. Prendiamo ora una *sezione*, cioè una *funzione*[36] $s\colon G \to E$ tale che $p \circ s = \mathrm{id}_G$. Definiamo un'azione[37] di G su $i(A)$ come

$$g \cdot i(a) \equiv s(g) i(a) s(g)^{-1}$$

[35] Ovviamente 1 indica il gruppo banale.

[36] E basta: anche questa non è necessariamente un omomorfismo.

[37] La verifica che questa è effettivamente un'azione, cioè che $(gh) \cdot i(a) = g \cdot (h \cdot i(a))$, può essere reperita a pagina 105 di [4].

che funziona perché $i(A)$ è normale. Quest'azione non dipende dalla scelta della sezione s: se infatti ne scegliamo un'altra e la battezziamo t, abbiamo $p(s(g)) = p(t(g))$, per cui $p(t(g)^{-1}s(g)) = 1$. Allora $t(g)^{-1}s(g) \in \operatorname{Ker} p = \operatorname{Im} i$ e quindi $t(g)^{-1}s(g) = i(a')$ per un certo a'. Dunque $s(g) = t(g)i(a')$ e

$$s(g)i(a)s(g)^{-1} = t(g)\underbrace{i(a')i(a)(i(a'))^{-1}}_{=i(a)}t(g)^{-1} = t(g)i(a)t(g)^{-1}$$

dove l'uguaglianza nella parentesi graffa segue dall'abelianità di $i(A)$. Possiamo enunciare ora che

Definizione 8.16. Sia G un gruppo e A un G-modulo. Un'*estensione di G tramite A* è una successione esatta di gruppi

$$1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

dove l'azione di G su $i(A)$ descritta sopra coincide con l'azione di G su A data dalla sua struttura di G-modulo.

Osservazione 8.17. La successione esatta

$$1 \to A \to A \rtimes G \to G \to 1$$

è un'estensione.

Fra le estensioni c'è un concetto di isomorfismo, lo "stesso" che per le estensioni di moduli: due estensioni sono isomorfe se esiste ψ che fa commutare

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Anche se non facciamo in tempo a dimostrarlo, enunciamo il seguente

Teorema 8.18. $H^2(G, A)$ è in bigezione con le classi di equivalenza di estensioni di G tramite A.

Concludiamo con due note:

1. Se l'azione di G su A è quella banale, cioè $s(g)i(a)s(g)^{-1} = i(a)$, allora $H^2(G, A)$ classifica le estensioni *centrali*, cioè quelle in cui $A \subset Z(E)$.
2. Se G ed A sono gruppi abeliani possiamo prendere un'estensione (notazione additiva) $0 \to A \to E \to G \to 0$ di quelle classificate da $\operatorname{Ext}^1_{\mathbb{Z}}(G, A)$, notare che è per forza centrale per abelianità, pensare A

come G-modulo banale e identificarla con la classe di equivalenza in $H^2(G, A) = \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ di (notazione moltiplicativa)

$$1 \to A \to E \to G \to 1$$

La domanda è: $\mathrm{Ext}^1_{\mathbb{Z}}(G, A)$ esaurisce tutte le estensioni centrali, ossia quelle che saltano fuori considerando l'azione di G su A banale e calcolando $H^2(G, A)$? La risposta è: no!

Esempio 8.19 (Perfido)**.** Consideriamo

$$1 \to \underbrace{\{\pm 1\}}_{A} \to Q_8 \to \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{G} \to 1$$

dove Q_8 sono i quaternioni e l'azione di G su A è quella banale.

Questa è "conteggiata" da $H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2)$, ma non da $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2)$ perché non è abeliana.

Appendice A

Alcuni Esercizi (e qualche soluzione)

Questa appendice contiene gli esercizi, alcuni dei quali muniti di soluzione, assegnati durante il corso in sostituzione della prova scritta. Le soluzioni, e conseguentemente gli errori, sono mie salvo che per l'Esercizio A.10, che mi sono limitato ad editare lievemente[1]. Alcune soluzioni sono *decisamente* più dettagliate del dovuto, per cui non fatevi spaventare dalla lunghezza.

A.1 A.A. 2014/2015

Esercizio A.1 (ripasso sul Nullstellensatz)**.** Come si dimostra, a partire dal Teorema 1.19, che dato un ideale I proprio in $\mathbb{K}[X_1, \ldots, X_n]$, il suo luogo di zeri $V(I)$ in $\overline{\mathbb{K}}^n$ non è vuoto?

Esercizio A.2. Siano $A = \dfrac{\mathbb{C}[x, y, z]}{(y^2 - x^3 - x^2)}$ e $B = \mathbb{C}[t, z]$. Dimostrare che:

a) A si può immergere come sottoanello di B tramite la mappa f definita da $f(\overline{x}) = t^2 - 1$, $f(\overline{y}) = t^3 - t$, $f(\overline{z}) = z$;

b) A e B hanno lo stesso campo dei quozienti;

c) $I = (t + 1, z - 1)$ è primo in B;

d) $J = (t^2 - 1, t^3 - t, z - 1)$ e $H = (t^3 - t - z(t^2 - 1), t^2 - z^2)$ sono ideali primi di A e $H \subseteq J$;

e) $I \cap A = J$;

f) non esiste un ideale D primo tale che $D \cap A = H$ e $D \subseteq I$.

[1] Il che significa che anche lei è suscettibile di miei errori.

Soluzione. a) È sufficiente mostrare che, denotando per brevità $(y^2-x^3-x^2) = K$, per $\varphi\colon \mathbb{C}[x,y,z] \to \mathbb{C}[t,z]$ definita come f ma togliendo i "$-$" dalle variabili vale $\operatorname{Ker}\varphi = K$. Un conto diretto mostra che $K \subseteq \operatorname{Ker}\varphi$ perché il suo unico generatore è mappato in 0:

$$\begin{aligned}\varphi(y^2 - x^3 - x^2) &= (t^3 - t)^2 - (t^2 - 1)^3 - (t^2 - 1)^2 \\ &= t^6 - 2t^4 + t^2 - t^6 + 3t^4 - 3t^2 + 1 - t^4 + 2t^2 - 1 = 0\end{aligned}$$

Supponiamo per assurdo che l'inclusione sia stretta. Dato che sappiamo che $\dim_{\text{Krull}} \mathbb{C}[x,y,z] = 3$, vogliamo esibire, sotto l'ipotesi di assurdo, una catena di ideali primi

$$(0) \subsetneq K \subsetneq \operatorname{Ker}\varphi \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$$

Dato che siamo in un dominio e che ogni primo può essere esteso ad un massimale è sufficiente dunque mostrare che

[1] $y^2 - x^3 - x^2$ è irriducibile e dunque K è primo ($\mathbb{C}[x,y,z]$ è un UFD);

[2] $\operatorname{Ker}\varphi$ è primo;

[3] esiste un ideale primo non massimale $\mathfrak{p} \supsetneq \operatorname{Ker}\varphi$;

Mostriamolo:

[1] Supponiamo che $y^2-x^3-x^2 = pq$. Se $\deg_y p = 2$, in pq dovrebbero comparire[2] monomi della forma $cx^\alpha y^2$, ma questo non succede. Dunque ci basta mostrare che non è possibile che valga $\deg_y p = \deg_y q = 1$. Se così fosse, in $\mathbb{C}(x)[y]$ avremmo una fattorizzazione della forma

$$\left(y - \frac{q_1(x)}{s_1(x)}\right)\left(y - \frac{q_2(x)}{s_2(x)}\right)$$

e dunque varrebbe

$$y^2 - x^3 - x^2 = y^2 + \frac{q_1(x)q_2(x)}{s_1(x)s_2(x)} - \frac{q_1(x)s_2(x) + q_2(x)s_1(x)}{s_1(x)s_2(x)}y$$

tralasciando le (x) per brevità, deve dunque valere $q_1 s_2 = -q_2 s_1$, da cui

$$-x^3 - x^2 = \frac{q_1 q_2 s_1}{s_1^2 s_2} = -\frac{q_1^2 s_2}{s_1^2 s_2} = -\left(\frac{q_1}{s_1}\right)^2$$

ma $\deg_x\big((x^3+x^2)s_1^2\big)$ è dispari e $\deg_x(q_1^2)$ è pari.

[2] Il quoziente per $\operatorname{Ker}\varphi$ è un sottoanello di $\mathbb{C}[t,z]$, ed è quindi un dominio.

[2] Basta considerare i monomi di grado totale massimo in p e q.

[3] Basta considerare $\psi\colon \mathbb{C}[x,y,z] \to \mathbb{C}[t]$ definita come φ salvo che per $\psi(z) = 0$ e porre $\mathfrak{p} = \operatorname{Ker}\psi$. Che $\mathfrak{p} \supsetneq \operatorname{Ker}\varphi$ è ovvio; d'altra parte il quoziente per $\mathfrak{p}$ è un dominio in quanto sottoanello di $\mathbb{C}[t]$, e non è un campo perché, ad esempio, contiene $t^2 - 1$.

b) È ovvio che $Q(A) \subseteq Q(B)$. Per l'altra inclusione basta notare che, in $Q(A)$,

$$\frac{t^3 - t}{1} \cdot \frac{1}{t^2 - 1} = t$$

c) I è il nucleo dell'omomorfismo $\varphi\colon B \to \mathbb{C}$ definito da $\varphi(p(t,z)) = p(-1,1)$. Dato che φ è banalmente surgettiva (basta considerare i polinomi costanti), il quoziente B/I è un campo, e quindi I è addirittura massimale.

d) Sia $\psi\colon \mathbb{C}[x,y,z] \to \mathbb{C}[t]$ l'omomorfismo di $\mathbb{C}$-algebre definito da $\psi(x) = t^2 - 1$, $\psi(y) = t^3 - t$, $\psi(z) = 1$. Dato che $\operatorname{Ker}\psi \supseteq K$, lo possiamo fattorizzare come

$$\mathbb{C}[x,y,z] \xrightarrow{\varphi} A \xrightarrow{\vartheta} \mathbb{C}[t], \qquad \psi = \vartheta\circ\varphi$$

Dato che per costruzione $\operatorname{Ker}\vartheta = J$, il quoziente A/J è un sottoanello di $\mathbb{C}[t]$ ed è quindi un dominio. Dunque J è primo. Dato che il primo generatore di H è già scritto come combinazione dei generatori di J, per dire che $H \subseteq J$ basta scrivere

$$t^2 - z^2 = t^2 - 1 - (z+1)(z-1) \tag{A.1}$$

e ci resta da far vedere che H è primo. Per la (A.1), la contrazione $\varphi^{-1}(H) \subseteq \mathbb{C}[x,y,z]$ è $(y - zx, x - z^2 + 1)$, che è può essere equivalentemente scritto[3] come $(y - z^3 + z, x - z^2 + 1)$. In questa forma è facile vedere che coincide con il nucleo della mappa surgettiva $\mathbb{C}[x,y,z] \to \mathbb{C}[z]$ che associa $x \mapsto z^2 - 1$, $y \mapsto z^3 - z$, $z \mapsto z$. In conclusione abbiamo

$$A/H \cong {(\mathbb{C}[x,y,z]/K)}\big/{(\varphi^{-1}(H)/K)} \cong \mathbb{C}[z]$$

e $\mathbb{C}[z]$ è un dominio.

e) Sappiamo già che $J \subseteq A$. Inoltre $J \subseteq I$ perché $t^2 - 1 = (t+1)(t-1)$, e quindi ogni generatore di J è multiplo di un generatore di I. Questo mostra $J \subseteq I \cap A$. Viceversa sia $p \in I \cap A$. Possiamo scrivere

$$\underbrace{\gamma(t,z)(t^2-1) + \delta(t,z)(t^3 - t) + \overbrace{\lambda}^{\in\mathbb{C}}}_{\text{perché } p\in A} = p = \underbrace{\alpha(t,z)(t+1) + \beta(t,z)(z-1)}_{\text{perché } p\in I}$$

[3] Ad esempio notando che nel quoziente vale $x = z^2 - 1$.

Dato che t^2-1, t^3-t sono fra i generatori di J basta mostrare $\lambda = 0$. Se così non fosse sarebbe invertibile, e da

$$\lambda = \big[\alpha(t,z) - \gamma(t,z)(t-1) - \delta(t,z)(t^2-t)\big](t+1) + \beta(t,z)(z-1) \in I$$

avremmo l'assurdo $I = A$.

f) Se un ideale si contrae ad H deve includere l'estensione H^e. È sufficiente quindi mostrare che $H^e \not\subseteq I$. Dato che

$$H^e \ni t^3 - t - z(t^2-1) + z(t^2-z^2) = z - t$$

se fosse $H^e \subseteq I$ avremmo l'assurdo

$$I \ni (z-t) + (t+1) - (z-1) = 2 \qquad \square$$

Esercizio A.3. Siano $A \subseteq B$ anelli, con B intero su A. Dimostrare che

a) se $x \in A$ è invertibile in B, allora è invertibile anche in A

b) il radicale di Jacobson di A è la contrazione del radicale di Jacobson di B.

Esercizio A.4. Sia A un sottoanello dell'anello B, e sia C la chiusura integrale di A in B. Siano f, g polinomi monici in $B[X]$ tali che $f, g \in C[X]$.

a) Dimostrare che esiste un anello D tale che $B \subseteq D$ e entrambi i polinomi f e g si fattorizzano in $D[X]$ come prodotto di fattori di grado 1.

b) Dimostrare che f e g appartengono a $C[X]$.

Esercizio A.5. Dimostrare che, dato un numero intero $d < -2$ libero da quadrati e congruo a 2 o a 3 modulo 4, l'anello $\mathbb{Z}[\sqrt{d}]$ non è a ideali principali.

Esercizio A.6. Si considerino due anelli $A \subseteq B$ e sia B un A-modulo finitamente generato. Dimostrare che, dato un ideale primo $\mathfrak{p}$ di A, gli ideali primi $\mathfrak{q}$ di B tali che $\mathfrak{q} \cap A = \mathfrak{p}$ sono in numero finito.

Dimostrazione. Notiamo preliminarmente che, per il Teorema 1.4, B è un'estensione intera di A in quanto A-modulo finitamente generato. Ogni $\mathfrak{q}$ come nella tesi deve necessariamente contenere l'estensione $\mathfrak{p}^e$ di $\mathfrak{p}$. Per la nota corrispondenza fra ideali nei quozienti non è dunque restrittivo, quozientando A per $\mathfrak{p}$ e B per $\mathfrak{p}^e$, supporre che A sia un dominio e che $\mathfrak{p} = (0)$, e l'ipotesi che B sia intero su A è conservata nel passaggio al quoziente per la Proposizione 1.9. Poniamo $S = A \setminus \{0\}$ e consideriamo $S^{-1}A \subseteq S^{-1}B$, che è intera per la Proposizione 1.10. Se $\mathfrak{q}$ è tale che $\mathfrak{q} \cap A = (0)$, per definizione di S si ha $S \cap \mathfrak{q} = \emptyset$. Dato che per un noto Teorema S^{-1} è una bigezione fra i primi di B disgiunti da S e i primi di $S^{-1}B$, ci basta mostrare che gli ideali primi di $S^{-1}B$ che si contraggono a (0) in $S^{-1}A$ sono in numero finito. Per il

Corollario 1.16 se $\mathfrak{q}_1$, $\mathfrak{q}_2$ sono primi di B, $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$ e $\mathfrak{q}_2 \cap A = \mathfrak{q}_1 \cap A = (0)$ deve necessariamente essere $\mathfrak{q}_2 \neq \mathfrak{q}_1$. Ma allora, per ogni $\mathfrak{q}$ come nella tesi, ogni primo $\mathfrak{r} \supsetneq \mathfrak{q}$ deve contenere un elemento di S; di conseguenza $S^{-1}\mathfrak{r} = B$, per cui ogni $S^{-1}\mathfrak{q}$ è massimale[4]. Dato che $S^{-1}A$ è un campo ogni ideale proprio $S^{-1}B$, e in particolare ogni primo, si contrae a (0) in $S^{-1}A$ (gli altri elementi di $S^{-1}A$ sono invertibili), per cui per il ragionamento precedente $\dim_{\text{Krull}}(S^{-1}B) = 0$. Dato che $S^{-1}A$ è noetheriano in quanto campo e che $S^{-1}B$ è un $S^{-1}A$-modulo finitamente generato è anch'esso noetheriano. Per il Teorema di Caratterizzazione degli Anelli Artiniani dunque $S^{-1}B$ è artiniano, e per la Proposizione 3.2 i suoi ideali massimali, e in particolare gli $S^{-1}\mathfrak{q}$, sono in numero finito. □

Esercizio A.7. Si consideri l'anello di polinomi $\mathbb{C}[X, Y, Z]$ graduato nella maniera standard. Si considerino gli ideali (graduati) $I_1 = (x^3 + y^3 + z^3)$ e $I_2 = (x^3 + y^3 + z^3, x^2 + y^2 + z^2)$. Si calcolino le serie di Poincaré

$$P(I_1, t), P(I_2, t), P(\mathbb{C}[X, Y, Z]/I_1), P(\mathbb{C}[X, Y, Z]/I_2)$$

dove la funzione "lunghezza" λ è data da $\dim_{\mathbb{C}}$.

Soluzione. Poniamo $I_{1,n} = I_1 \cap \mathbb{C}[X, Y, Z]_n$. Per $n < 3$ si ha chiaramente $I_{1,n} = \{0\}$, dato che I_1 non contiene polinomi omogenei di grado minore di 3. Dato che l'ideale $I_1 = (p)$ è principale in un dominio, ogni suo elemento pq è univocamente determinato da q, e quindi per calcolare $\lambda(I_{1,n}) = \dim_{\mathbb{C}}(I_{1,n})$ per $n \geq 3$ è sufficiente contare i monomi di grado $n-3$ in 3 variabili. Questo è equivalente a contare in quanti modi $n-3$ può essere scritto come somma di 3 interi non negativi, e come noto tali modi sono $\binom{n-3+2}{2}$, per cui

$$P(I_1, t) = \sum_{n=3}^{\infty} \binom{n-1}{2} t^n$$

Inoltre, considerando la successione esatta corta

$$0 \to I_{1,n} \to \mathbb{C}[X, Y, Z]_n \to (\mathbb{C}[X, Y, Z]/I_1)_n \to 0$$

e, utilizzando l'additività di λ e convenendo che $\binom{n-1}{2} = 0$ se $n < 3$, si ottiene subito

$$P(\mathbb{C}[X, Y, Z]/I_1, t) = \sum_{n=0}^{\infty} \left(\binom{n+2}{2} - \binom{n-1}{2} \right) t^n = 1 + \sum_{n=1}^{\infty} 3nt^n$$

Per quanto riguarda $I_{2,n} = (p_3, p_2)_n$, per $n < 2$ si ha $\lambda(I_{2,n}) = 0$ e $\lambda(I_{2,2}) = 1$ per ovvi motivi, mentre per $n \geq 3$ possiamo scrivere ogni suo elemento come

[4] A patto che sia un ideale proprio, ma questo è vero perché $\mathfrak{q} \cap S = \emptyset$.

$p_3q_3 + p_2q_2$, con q_3 omogeneo di grado $n-3$ e q_2 omogeneo di grado $n-2$, ma questa volta la scrittura non è unica. Consideriamo la successione esatta

$$0 \to \operatorname{Ker}\varphi \to \mathbb{C}[X,Y,Z]_{n-3} \times \mathbb{C}[X,Y,Z]_{n-2} \to I_{2,n} \to 0$$

dove $\varphi(q_3, q_2) = p_3q_3 + p_2q_2$. Se $(q_3, q_2) \in \operatorname{Ker}\varphi$, dato che $\mathbb{C}[X,Y,Z]$ è un UFD e che sia p_3 che p_2 sono irriducibili deve valere $q_3 \mid p_2$ e $q_2 \mid p_3$, quindi si deve avere una situazione del tipo

$$0 = p_3q_3 + p_2q_2 = p_3p_2r$$

dove r è omogeneo del grado appropriato, cioè $n-5$. In definitiva, per $n \geq 5$,

$$\begin{aligned}\lambda(I_{2,n}) &= \lambda(\mathbb{C}[X,Y,Z]_{n-3} \times \mathbb{C}[X,Y,Z]_{n-2}) - \lambda(\underbrace{\operatorname{Ker}\varphi}_{\cong \mathbb{C}[X,Y,Z]_{n-5}}) \\ &= \binom{n-1}{2} + \binom{n}{2} - \binom{n-3}{2} = \frac{(n-2)(n+5)}{2}\end{aligned}$$

nei casi $n = 3, 4$ il ragionamento precedente mostra $\lambda(\operatorname{Ker}\varphi) = 0$, quindi in ultima analisi

$$P(I_2, t) = t^2 + 4t^3 + 9t^4 + \sum_{n=5}^{\infty} \frac{(n-2)(n+5)}{2} t^n = \sum_{n=3}^{\infty} \frac{(n-2)(n+5)}{2} t^n$$

e, analogamente a prima, convenendo $(n-2)(n+5) = 0$ se $n < 3$,

$$\begin{aligned}P(\mathbb{C}[X,Y,Z]/I_2, t) &= \sum_{n=0}^{\infty} \left(\binom{n+2}{2} - \frac{(n-2)(n+5)}{2} \right) t^n \\ &= 1 + 3t + 5t^2 + \sum_{n=3}^{\infty} 6t^n \quad \square\end{aligned}$$

Esercizio A.8. Sia A un anello completo rispetto alla topologia indotta da un ideale I. Sia (a_n) una successione in A. Dimostrare che la serie $\sum_{n=0}^{\infty} a_n$ converge se e solo se $\lim_{n\to\infty} a_n = 0$.

Soluzione. Se $\sum_{n=0}^{\infty} a_n$ converge deve essere di Cauchy, e quindi per ogni j definitivamente vale

$$\sum_{n=0}^{\mu} a_n - \sum_{n=0}^{\nu} a_n = \sum_{n=\nu}^{\mu} a_n \in I^j$$

In particolare questo è vero per $\mu = \nu$, e dunque a_n sta definitivamente in I^j. Siccome $\{I^j \mid j \in \mathbb{N}\}$ è un sistema fondamentale di intorni di 0 abbiamo provato che $\lim_{n\to\infty} a_n = 0$.

Viceversa, fissato j, sia N tale che per $n \geq N$ si abbia $a_n \in I^j$. Allora per ogni $\mu, \nu \geq N$ si ha

$$\sum_{n=0}^{\mu} a_n - \sum_{n=0}^{\nu} a_n = \sum_{n=\nu}^{\mu} a_n \in I^j$$

in quanto I^j è un ideale e in particolare un sottogruppo additivo. Dunque la successione delle somme parziali è di Cauchy e converge perché siamo in uno spazio completo. □

Esercizio A.9. Sia A un dominio e I un ideale di A. Denotiamo con $\mathrm{gr}(A)$ l'anello graduato associato ad A rispetto alla filtrazione indotta da I e con $\hat{A}_I$ il completamento di A rispetto alla topologia I-adica.

a) È vero o falso che A dominio implica $\mathrm{gr}(A)$ dominio? E il viceversa?

b) Nell'Esercizio 4.9 abbiamo visto che non è vero che A dominio implica $\hat{A}_I$ dominio. E il viceversa?

Soluzione. a) Nessuna delle due implicazioni è vera:

- A dominio non implica $\mathrm{gr}(A)$ dominio: basta prendere $A = \mathbb{Z}$ e $I = 6\mathbb{Z}$. In $\mathrm{gr}(A) = \bigoplus_{j=0}^{\infty} I^j/I^{j+1}$ si ha

$$(2, 0, 0, 0, \ldots) \cdot (3, 0, 0, 0 \ldots) = (0, 0, 0, 0 \ldots)$$

- $\mathrm{gr}(A)$ dominio non implica A dominio: basta prendere $A = \mathbb{Z}/6\mathbb{Z}$ e $I = 3\mathbb{Z}/6\mathbb{Z}$. Dato che $I^2 = I$ si ha $\mathrm{gr}(A) \cong \mathbb{Z}/3\mathbb{Z}$.

b) È falso: anche qui basta prendere $A = \mathbb{Z}/6\mathbb{Z}$ e $I = 3\mathbb{Z}/6\mathbb{Z}$. La filtrazione è

$$A = \mathbb{Z}/6\mathbb{Z} \supseteq {}^{\mathbb{Z}/6\mathbb{Z}}\!/_{3\mathbb{Z}/6\mathbb{Z}} \supseteq {}^{\mathbb{Z}/6\mathbb{Z}}\!/_{3\mathbb{Z}/6\mathbb{Z}} \supseteq \cdots \supseteq {}^{\mathbb{Z}/6\mathbb{Z}}\!/_{3\mathbb{Z}/6\mathbb{Z}} \supseteq \cdots$$

e per la condizione di compatibilità tutte le g_n sono l'identità, per cui è immediato notare che $\hat{A}_I \cong \mathbb{Z}/3\mathbb{Z}$. □

La soluzione dell'Esercizio seguente è di G. Inchiostro, G. M. Lido e C. Sircana.

Esercizio A.10. Sia A un anello locale noetheriano con ideale massimale $\mathfrak{m}$ e sia $\mathfrak{q}$ un ideale $\mathfrak{m}$-primario. Allora $\dim(A) = \dim(\mathrm{gr}_{\mathfrak{q}}(A))$.

Soluzione. Questa è una di quelle cose di cui si capisce il senso alla fine, perché l'inizio è pieno di tecnicismi. Per provare a rimediare, spoileriamo subito che la dimostrazione finirà con questa riga:

$$\dim(\mathrm{gr}_{\mathfrak{q}}(A)) = \dim((\mathrm{gr}_{\mathfrak{q}}(A))_P) = \mathrm{OP}(\mathrm{gr}_{Q^e}((\mathrm{gr}_{\mathfrak{q}}(A))_P)) = \mathrm{OP}(\mathrm{gr}_{\mathfrak{q}}(A)) = \dim A$$

che riporto all'inizio perché spero renda più comprensibili le parole "l'idea è localizzare in maniera furba per poi rigraduare in maniera da trasformare dim in OP." Comunque, se è ancora tutto incomprensibile, il lettore può passare oltre e tuffarsi nei dettagli senza paura di essersi perso niente.

Entriamo nel tecnico. Innanzitutto indaghiamo sui primi minimali degli anelli graduati. Se B un anello graduato e I è un ideale di B definiamo

$$I^h = \bigoplus_{n\in\mathbb{N}} I \cap B_i$$

I^h è per definizione un ideale omogeneo[5] ed è il più grande ideale omogeneo contenuto in I. Inoltre, per gli ideali omogenei, il "test di primalità" può essere fatto ristretto a elementi omogenei, cioè se per ogni a, b elementi omogenei vale $ab \in I^h \Rightarrow (a \in I^h \ \vee \ b \in I^h)$ allora I^h è un ideale primo[6]. Usando questo fatto è facile vedere che allora se I è primo lo è anche I^h. Dato che $I^h \subseteq I$, ne segue subito che se I è un primo minimale coincide con I^h. In sostanza abbiamo mostrato che

Fatto. I primi minimali di un anello graduato sono omogenei.

Restringiamoci ora al caso particolare dell'anello graduato.

$$\mathrm{gr}_{\mathfrak{q}}(A) = {}^{A}\!/_{\mathfrak{q}} \oplus {}^{\mathfrak{q}}\!/_{\mathfrak{q}^2} \oplus {}^{\mathfrak{q}^2}\!/_{\mathfrak{q}^3} \oplus \dots$$

Quozientando per un qualsiasi ideale primo minimale I, si ottiene un dominio graduato; dato che un sottoanello di un dominio è un dominio, in particolare questo deve valere per il sottoanello degli elementi di grado 0. Visto che l'anello $A/\mathfrak{q}$ è locale di dimensione 0, il quoziente $\mathrm{gr}_{\mathfrak{q}}(A)/I$ è una $\mathbb{K}$-algebra finitamente generata che è anche un dominio, e tutti i suoi ideali massimali hanno allora la stessa altezza per il Corollario 2.9. Questo vale per ogni ideale minimale di $\mathrm{gr}_{\mathfrak{q}}(A)$, dunque è sufficiente calcolare l'altezza dell'ideale omogeneo

$$P = {}^{\mathfrak{m}}\!/_{\mathfrak{q}} \oplus {}^{\mathfrak{q}}\!/_{\mathfrak{q}^2} \oplus {}^{\mathfrak{q}^2}\!/_{\mathfrak{q}^3} \oplus \dots$$

che contiene tutti i primi minimali, perché questi ultimi sono omogenei[7]. Per calcolare questo, localizziamo $\mathrm{gr}_{\mathfrak{q}}(A)$ rispetto all'ideale P e calcoliamo il graduato rispetto all'ideale

$$Q = \left((0) \oplus {}^{\mathfrak{q}}\!/_{\mathfrak{q}^2} \oplus {}^{\mathfrak{q}^2}\!/_{\mathfrak{q}^3} \oplus \dots\right)^e$$

[5] Vuol dire che ha generatori omogenei o, equivalentemente, che se $x \in I^h$ allora tutte le componenti omogenee di x stanno in I^h.

[6] Questo è facile da vedere spezzando un elemento in componenti omogenee.

[7] Provate a pensare dove possono vivere (cioè che grado possono avere) i loro generatori...

Otteniamo quindi

$$\mathrm{gr}_{Q^e}\big((\mathrm{gr}_{\mathfrak{q}}(A))_P\big) = {(\mathrm{gr}_{\mathfrak{q}}(A))_P}\big/{Q^e} \oplus {Q^e}\big/{(Q^e)^2} \oplus \dots$$

Sorprendentemente $(\mathrm{gr}_{\mathfrak{q}}(A))_P/Q^e \cong A/\mathfrak{q}$ e $(Q^e)^n/(Q^e)^{n+1} \cong \mathfrak{q}^n/\mathfrak{q}^{n+1}$, da cui l'isomorfismo

$$\mathrm{gr}_{Q^e}((\mathrm{gr}_{\mathfrak{q}}(A))_P) \cong \mathrm{gr}_{\mathfrak{q}}(A)$$

E, come promesso all'inizio, la dimostrazione finisce scrivendo

$$\dim(\mathrm{gr}_{\mathfrak{q}}(A)) = \dim((\mathrm{gr}_{\mathfrak{q}}(A))_P) = \mathrm{op}(\mathrm{gr}_{Q^e}((\mathrm{gr}_{\mathfrak{q}}(A))_P)) = \mathrm{op}(\mathrm{gr}_{\mathfrak{q}}(A)) = \dim A$$

□

Esercizio A.11. Si consideri l'anello $A = \mathbb{Z}[\sqrt{-3}]$. Dimostrare che l'ideale $\mathfrak{m} = (2, 1+\sqrt{-3})$ è massimale. L'anello locale $A_{\mathfrak{m}}$ è regolare?

Soluzione. L'ideale $\mathfrak{m}$ è massimale perché coincide col nucleo dell'omomorfismo surgettivo $\varphi\colon A \to \mathbb{F}_2$ definito come

$$\varphi(a + b\sqrt{-3}) = [a+b]_2$$

Che φ commuti con la somma e mandi 1 in $[1]_2$ è ovvio, mentre φ commuta col prodotto perché

$$\begin{aligned}\varphi\big((a+b\sqrt{-3})(c+d\sqrt{-3})\big) &= \varphi\big((ac-3bd)+(bc+ad)\sqrt{-3}\big)\\ &= [ac+bd+bc+ad]_2 = [a+b]_2[c+d]_2 = \varphi(a+b\sqrt{-3})\varphi(c+d\sqrt{-3})\end{aligned}$$

Inoltre $\mathfrak{m} \subseteq \operatorname{Ker}\varphi$ perché $\varphi(2) = \varphi(1+\sqrt{-3}) = 0$. Viceversa, se $\varphi(a + b\sqrt{-3}) = 0$, allora a è b hanno la stessa parità. Se $a = 2m$ e $b = 2n$ allora

$$a + b\sqrt{-3} = 2m + 2n\sqrt{-3} = (m-n)\cdot 2 + 2n\cdot(1+\sqrt{-3}) \in \mathfrak{m}$$

mentre se $a = 2m+1$ e $b = 2n+1$ allora risulta

$$a+b\sqrt{-3} = (2m+1)+(2n+1)\sqrt{-3} = (m-n)\cdot 2 + (2n+1)\cdot(1+\sqrt{-3}) \in \mathfrak{m}$$

e dunque $\operatorname{Ker}\varphi \subseteq \mathfrak{m}$.

L'anello $A_{\mathfrak{m}}$ non è regolare: per il Teorema 5.25 è infatti sufficiente mostrare che $\dim_{A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}}(\mathfrak{m}_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2) \neq \dim(A_{\mathfrak{m}})$. Ora $\dim(A) = \dim(\mathbb{Z}) = 1$ perché A è un'estensione intera di $\mathbb{Z}$; dunque $\dim A_{\mathfrak{m}} \leq 1$, e dato che $A_{\mathfrak{m}}$ è un dominio ma non un campo $\dim A_{\mathfrak{m}} = 1$.

Dato che $A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} \cong A/\mathfrak{m} \cong \mathbb{F}_2$, è sufficiente mostrare che in $\mathfrak{m}_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^2$ ci sono tre elementi distinti. Dato che $\mathfrak{m}^2 = (4, 2+2\sqrt{-3}, 2-2\sqrt{-3}) = (4, 2+2\sqrt{-3})$, tali tre elementi sono

$$\frac{[0]_{\mathfrak{m}^2}}{1} \qquad \frac{[2]_{\mathfrak{m}^2}}{1} \qquad \frac{[1+\sqrt{-3}]_{\mathfrak{m}^2}}{1}$$

dove gli ultimi due sono distinti perché se fosse $1+\sqrt{-3}-2 = -1+\sqrt{-3} \in \mathfrak{m}^2$ dovrebbe essere

$$-1+\sqrt{-3} = (a+b\sqrt{-3})\cdot 4+(c+d\sqrt{-3})\cdot(2+2\sqrt{-3}) = (4a+2c-6d)+(\ldots)\cdot\sqrt{-3}$$

e ci sono evidenti problemi di parità. □

Esercizio A.12. Sia A la localizzazione di $\mathbb{Z}[x,y]$ nell'ideale massimale $(5, x-1, y+2)$ e sia $B = A/(x^2+y^2+4y-3x+6)$. Stabilire se B è un anello locale regolare.

Soluzione. Sappiamo dal Teorema 5.34 che $\dim \mathbb{Z}[x,y] = 3$, dunque $\dim A \leq 3$, e una catena che testimonia l'altra disuguaglianza è

$$(0) \subsetneq (5) \subsetneq (5, x-1) \subsetneq (5, x-1, y+2)$$

Sappiamo che A è locale noetheriano, che $q = x^2+y^2+4y-3x+6$ non è uno 0-divisore (A è un dominio) e che $q \in (5, x-1, y+2)^e$ perché[8]

$$q = x^2+y^2+4y-3x+6 = (y+2)^2+(x-2)(x-1)$$

Dunque per il Corollario 5.19 $\dim B = \dim A - 1 = 2$. Ora B è noetheriano perché quoziente di un noetheriano, ed è locale per la corrispondenza fra ideali nei quozienti. Per la regolarità basta mostrare che l'ideale massimale di B è generato da 2 elementi. Tuttavia in B vale[9]

$$(x-1) = \frac{(y+2)^2}{2-x}$$

e quindi 5 e $y+2$ sono sufficienti a generare il suo ideale massimale. □

Esercizio A.13. Sia A un dominio noetheriano locale con ideale massimale $\mathfrak{m}$. Sia $B = A[X]_{\mathfrak{q}}$ dove $\mathfrak{q}$ è un ideale primo di $A[X]$ tale che $\mathfrak{m}[X] \subseteq \mathfrak{q}$. Dimostrare che

$$\dim B = \dim A + 1 - \operatorname{tr}_{\deg} k'/k$$

dove $k = A/\mathfrak{m}$ e k' è il campo residuo di B (e $k \subseteq k'$ in modo ovvio).

Soluzione. Mostriamo preliminarmente che $\dim B/\mathfrak{m}B$ può essere solo 0 o 1. Se ciò fosse falso, per la nota corrispondenza fra primi negli anelli di frazioni avremmo una catena $\mathfrak{p}_1^c \supsetneq \mathfrak{p}_0^c \supsetneq \mathfrak{m}[X]$ di primi di $A[X]$ che si contraggono tutti ad $\mathfrak{m}$ per massimalità di quest'ultimo, e per l'Esercizio 5.30, se A ha dimensione finita, questo non può succedere. Tuttavia A è noetheriano locale e quindi ha dimensione finita per il Corollario 5.12.

[8] Identificando $\frac{a}{1}$ con a.

[9] Per evitare di appesantire la notazione confonderemo liberamente a con $\left[\frac{a}{1}\right]_{(q)}$.

Mostriamo la disuguaglianza "$\leq$". È chiaro che B è noetheriano locale, e la naturale mappa $A \to B$ è locale per ipotesi. Siamo dunque nelle ipotesi del Teorema della Dimensione della Fibra, per cui

$$\dim B \leq \dim A + \dim {}^{B}\!/_{\mathfrak{m}B}$$

Ora mostriamo che $\dim(B/\mathfrak{m}B) = 1 - \mathrm{tr}_{\deg}(k'/k)$. Forti della nostra osservazione preliminare, procediamo per casi a seconda del valore di $\dim B/\mathfrak{m}B$:

0. In questo caso, dato che $\mathfrak{m}B$ è primo, $B/\mathfrak{m}B$ è un dominio di dimensione 0 e quindi un campo. Dunque $\mathfrak{m}B$ è massimale e l'inclusione $\mathfrak{m}B \subseteq \mathfrak{q}_{\mathfrak{q}}$ è in realtà un'uguaglianza, e per la solita corrispondenza fra primi negli anelli di frazioni vale dunque $\mathfrak{m}[X] = \mathfrak{q}$. Ma allora k' è il campo delle frazioni di $A[X]/\mathfrak{m}[X]$, cioè $(A/\mathfrak{m})(X) = k(X)$, ed è dunque palese che $\mathrm{tr}_{\deg}(k'/k) = 1$.

1. In questo caso, sempre per la solita corrispondenza, in $A[X]$ abbiamo $\mathfrak{m}[X] \subsetneq \mathfrak{q}$; inoltre, tramite ripetute iterazioni del Going Down Piatto, che può essere utilizzato perché $A[X]$ è un A-modulo piatto[10] e perché lo noetherianità si conserva nelle iterazioni per il Teorema della Base di Hilbert, $\mathfrak{m}[X]$ ha altezza $\dim A$, e dato che $A[X]$ ha dimensione $\dim A + 1$ per il Teorema 5.34, l'ideale $\mathfrak{q}$ è massimale. Ne segue che $A[X]/\mathfrak{q} \cong B/\mathfrak{q}_{\mathfrak{q}} = k'$. La situazione è quindi

$$k = {}^{A}\!/_{\mathfrak{m}} \hookrightarrow \frac{(A[X]/\mathfrak{m}[X])}{(\mathfrak{q}/\mathfrak{m}[X])} \cong {}^{A[X]}\!/_{\mathfrak{q}} \cong {}^{B}\!/_{\mathfrak{q}_{\mathfrak{q}}} = k'$$

   Ma l'estensione di campi ai lati della freccia $\hookrightarrow$ è chiaramente algebrica e dunque $\mathrm{tr}_{\deg}(k'/k) = 0$.

Mostriamo la disuguaglianza "$\geq$". Consideriamo una catena di primi di A di lunghezza $\dim A$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{\dim(A)-1} \subsetneq \mathfrak{m}$$

trasportiamola nella catena di primi di $A[X]$

$$\mathfrak{p}_0[X] \subsetneq \mathfrak{p}_1[X] \subsetneq \ldots \subsetneq \mathfrak{p}_{\dim(A)-1}[X] \subsetneq \mathfrak{m}[X]$$

e produciamo infine, ancora usando la solita corrispondenza fra primi, una catena di primi di B

$$(\mathfrak{p}_0[X])_{\mathfrak{q}} \subsetneq (\mathfrak{p}_1[X])_{\mathfrak{q}} \subsetneq \ldots \subsetneq (\mathfrak{p}_{\dim(A)-1}[X])_{\mathfrak{q}} \subsetneq (\mathfrak{m}[X])_{\mathfrak{q}} = \mathfrak{m}B$$

Se $\dim(B/\mathfrak{m}B) = 1 - \mathrm{tr}_{\deg}(k'/k) = 0$ abbiamo concluso. Se invece siamo nel caso in cui $\dim(B/\mathfrak{m}B) = 1$ vuol dire che esiste un primo $\mathfrak{p} \supsetneq \mathfrak{m}B$, e basta usarlo per allungare la catena. □

[10] Vedi Esercizio 5 del Capitolo II di [2].

Esercizio A.14. Consideriamo l'ideale $I = (2, X)$ in $\mathbb{Z}[X]$. Trovare un omomorfismo di $\mathbb{Z}[X]$-moduli da I a $\mathbb{Q}[X]/\mathbb{Z}[X]$ che non si estende a tutto $\mathbb{Z}[X]$. [Dunque lo $\mathbb{Z}[X]$-modulo $\mathbb{Q}[X]/\mathbb{Z}[X]$ non è iniettivo.]

Soluzione. Definiamo $\varphi\colon I \to \mathbb{Q}[X]/\mathbb{Z}[X]$ come

$$\varphi(p(X)\cdot 2 + q(X)\cdot X) = \left[q(X)\cdot\frac{X+1}{2}\right]_{\mathbb{Z}[X]}$$

È chiaro che $\varphi((p\cdot 2+q\cdot X)+(\bar{p}\cdot 2+\bar{q}\cdot X)) = \varphi(p\cdot 2+q\cdot X)+\varphi(\bar{p}\cdot 2+\bar{q}\cdot X)$ e che $\varphi(r\cdot(p\cdot 2+q\cdot X)) = r\cdot\varphi(p\cdot 2+q\cdot X)$. Tuttavia, dato che I non è uno $\mathbb{Z}[X]$-modulo libero, bisogna mostrare che φ è ben definita. Intanto notiamo che $\varphi(2X) = 0$ sia che scriviamo $2X = X\cdot 2+0\cdot X$ sia che scriviamo $2X = 0\cdot 2+2\cdot X$. Ora, se $p\cdot 2+q\cdot X = \tilde{p}\cdot 2+\tilde{q}\cdot X$ allora $(p-\tilde{p})\cdot 2+(q-\tilde{q})\cdot X = 0$. Dato che $\mathbb{Z}[X]$ è un UFD allora deve essere $X \mid (p-\tilde{p})$ e $2 \mid (q-\tilde{q})$. Dunque $(p-\tilde{p})\cdot 2+(q-\tilde{q})\cdot X = s\cdot 2X$; ma allora, dato che $\varphi(2X) = 0$, abbiamo $\varphi((p-\tilde{p})\cdot 2+(q-\tilde{q})\cdot X) = \varphi(s\cdot 2X) = s\cdot\varphi(2X) = 0$ e φ è ben definita.

Se, per assurdo, φ si estendesse a $\tilde{\varphi}\colon \mathbb{Z}[X] \to \mathbb{Z}[X]/\mathbb{Q}[X]$, avremmo

$$\left[\frac{X+1}{2}\right]_{\mathbb{Z}[X]} = \varphi(X) = \tilde{\varphi}(X) = \tilde{\varphi}(X\cdot 1) = X\cdot\tilde{\varphi}(1)$$

Questo è assurdo perché, fissato un rappresentante $\sum_{i=0}^{n}\frac{a_i}{b_i}X^i$ per $\tilde{\varphi}(1)$,

$$0 = \left[\frac{X+1}{2}\right]_{\mathbb{Z}[X]} - X\cdot\tilde{\varphi}(1) = \left[\frac{X+1}{2} - \sum_{i=0}^{n}\frac{a_i}{b_i}X^{i+1}\right]_{\mathbb{Z}[X]}$$

ma il termine di grado 0 dell'espressione a destra fra quadre è $1/2 \notin \mathbb{Z}[X]$. □

Esercizio A.15. Sia $\mathcal{B}$ la categoria i cui oggetti sono gli insiemi finiti e i cui morfismi sono le bigezioni. Sia $\mathcal{S}$ la categoria degli insiemi. Consideriamo i seguenti due funtori, Sym e Ord, da $\mathcal{B}$ a $\mathcal{S}$. Per ogni oggetto X di $\mathcal{B}$, $\mathrm{Sym}(X)$ è l'insieme delle bigezioni da X in sé, e $\mathrm{Ord}(X)$ è l'insieme di tutti gli ordini totali che si possono mettere in X (=liste ordinate di lunghezza uguale alla cardinalità di X). Per ogni morfismo $f \in \mathcal{B}[X, Y]$, $\mathrm{Sym}(f)$ è il morfismo che manda $\sigma \in \mathrm{Sym}(X)$ in $f\circ\sigma\circ f^{-1} \in \mathrm{Sym}(Y)$ e $\mathrm{Ord}(f)$ è il morfismo che manda la lista $(x_1, x_2, \ldots)$ nella lista $(f(x_1), f(x_2), \ldots)$.

Verificare che Sym e Ord sono ben definiti. Sono naturalmente equivalenti?

Soluzione. Verifichiamo che le due mappe sono effettivamente funtori: Occupiamoci prima di Sym:

- $\mathrm{Sym}(\mathrm{id}_X)$ e la mappa che associa ogni σ a $\mathrm{id}_X\circ\sigma\circ\mathrm{id}_X^{-1} = \sigma$. Dunque $\mathrm{Sym}(\mathrm{id}_X) = \mathrm{id}_{\mathrm{Sym}(X)}$.

- $\mathrm{Sym}(f \circ_{\mathcal{B}} g)$ è la mappa $\sigma \mapsto fg\sigma g^{-1}f^{-1}$. D'altra parte

$$(\mathrm{Sym}(f)) \circ_{\mathcal{S}} (\mathrm{Sym}(g)) = (\tau \mapsto f\tau f^{-1}) \circ_{\mathcal{S}} (\sigma \mapsto g\sigma g^{-1}) = (\sigma \mapsto f \underbrace{g\sigma g^{-1}}_{\tau} f^{-1})$$

Ora è il turno di Ord:

- $\mathrm{Ord}(\mathrm{id}_X) = \big((x_1, \dots, x_n) \mapsto (\mathrm{id}_X(x_1), \dots, \mathrm{id}_X(x_n)) = (x_1, \dots, x_n)\big) = \mathrm{id}_{\mathrm{Ord}(X)}$
- Da un lato $\mathrm{Ord}(f \circ_{\mathcal{B}} g) = \big((x_1, \dots, x_n) \mapsto (fg(x_1), \dots, fg(x_n))\big)$. Dall'altro $(\mathrm{Ord}(f)) \circ_{\mathcal{S}} (\mathrm{Ord}(g))$ è uguale a

$$\begin{aligned}&\big((y_1, \dots, y_n) \mapsto (f(y_1), \dots, f(y_n))\big) \circ_{\mathcal{S}} \big((x_1, \dots, x_n) \mapsto (g(x_1), \dots, g(x_n))\big) \\ &= \big((x_1, \dots, x_n) \mapsto (f\underbrace{g(x_1)}_{y_1}, \dots, f\underbrace{g(x_n)}_{y_n})\big)\end{aligned}$$

I due funtori non sono naturalmente equivalenti. Per mostrarlo supponiamo che esista $\tau\colon \mathrm{Sym} \to \mathrm{Ord}$ equivalenza naturale, e fissiamo $X \in \mathcal{B}$ e $\sigma \in \mathrm{Sym}(X)$ tale che $\sigma \neq \mathrm{id}_X$ (perché σ esista basta che $|X| \geq 2$). Per ogni $f \in \mathcal{B}[X, X]$ dalla commutatività del diagramma

$$\begin{array}{ccc} \mathrm{Sym}(X) & \overset{\tau_X}{\to} & \mathrm{Ord}(X) \\ {\scriptstyle \mathrm{Sym}(f)}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \mathrm{Ord}(f)} \\ \mathrm{Sym}(X) & \underset{\tau_X}{\to} & \mathrm{Ord}(X) \end{array}$$

segue che[11] per ogni $i \in \{1, \dots, |X|\}$, denotando $(x_1, \dots, x_n)_i = x_i$,

$$f((\tau_X(\sigma))_i) = (\tau_X(f\sigma f^{-1}))_i$$

Ora poniamo[12] $f = \sigma$ e sostituendo otteniamo

$$\sigma((\tau_X(\sigma))_i) = (\tau_X(\sigma\sigma\sigma^{-1}))_i = (\tau_X(\sigma))_i$$

Questo vale per ogni i, dunque per ogni elemento della lista $\tau_X(\sigma)$, cioè per ogni elemento di X. Dunque $\sigma = \mathrm{id_X}$, contro la scelta di σ. □

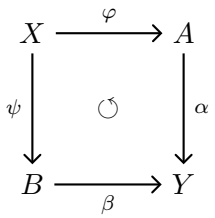
[11] Questo semplicemente perché due liste sono uguali se e solo se hanno la stessa lunghezza e lo sono in tutte le posizioni.

[12] Qui sembra che ci sia un lieve abuso di notazione dovuto all'identificare $\mathrm{Sym}(X)$ con $\mathcal{B}(X, X)$. In realtà i due coincidono, ma in caso l'identificazione non piaccia, sostituire "Poniamo $f = \sigma$" con "Sia $f \in \mathcal{B}[X, X]$ la bigezione $X \to X$ che come mappa insiemistica coincide con $\sigma \in \mathrm{Sym}(X)$".

Esercizio A.16. Enunciare e dimostrare i duali del Lemma 7.33 e del Lemma 7.34.

Soluzione.

Lemma A.17. Se il quadrato



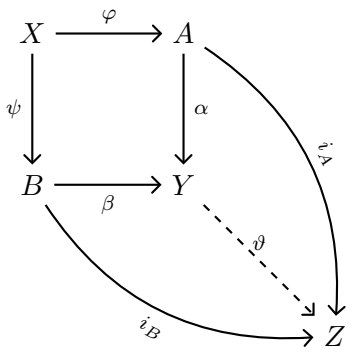
è un pushout allora

1. β induce un isomorfismo fra $\operatorname{Coker}\alpha$ e $\operatorname{Coker}\psi$

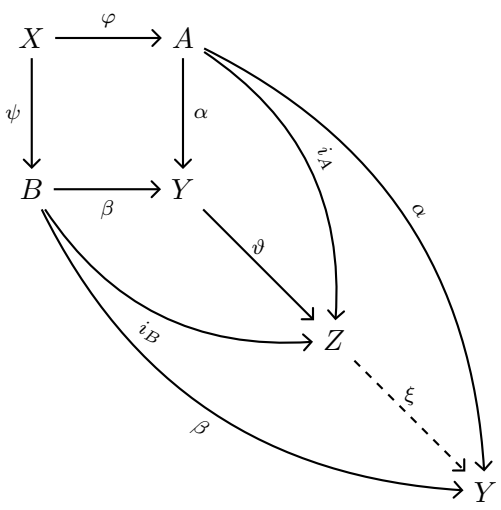
2. Se ψ è iniettiva allora α è iniettiva

Dimostrazione.

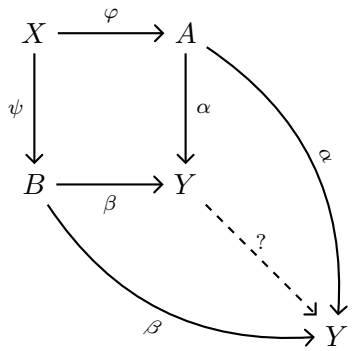
1. Sia $Z = (A \oplus B)/\operatorname{Im}\langle\varphi, -\psi\rangle$ il pushout costruito esplicitamente, e denotiamo le sue mappe con i_A e i_B. Invocando la proprietà di pushout su Y otteniamo ϑ che fa commutare



Per prima cosa mostriamo che ϑ è un isomorfismo: infatti possiamo disegnare il diagramma



dove ξ è ottenuta applicando la proprietà di pushout a Z. Un ulteriore utilizzo della proprietà di pushout ci fornisce

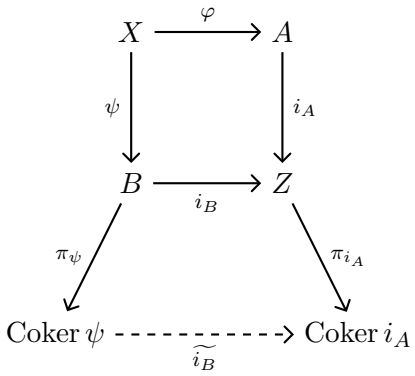


e al posto del "?" ci possiamo mettere sia id_Y che $\xi \circ \vartheta$, ma per definizione la mappa che va al posto del "?" è unica. Ripetendo il ragionamento scambiando i ruoli di Y e di Z si ottiene anche $\vartheta \circ \xi = \mathrm{id}_Z$, per cui ϑ è un isomorfismo.

Ne consegue che, opportunamente passata ai quozienti, ϑ induce un isomorfismo fra $\operatorname{Coker} \alpha$ e $\operatorname{Coker} i_A$. Infatti, da $i_A = \vartheta \circ \alpha$, otteniamo

$$\operatorname{Coker} i_A = \frac{Z}{\operatorname{Im} \vartheta \circ \alpha} \cong \frac{\vartheta^{-1}(Z)}{\operatorname{Im} \vartheta^{-1} \circ \vartheta \circ \alpha} = \operatorname{Coker} \alpha$$

Possiamo quindi, a meno di isomorfismo, lavorare su $\operatorname{Coker} i_A$. Per commutatività $i_B(\operatorname{Im} \psi) \subseteq \operatorname{Im} i_A$, e quindi i_B induce una $\widetilde{i_B}$ fra i quozienti come in figura:



Mostriamo che $\widetilde{i_B}$ è un isomorfismo. Per definizione $\operatorname{Im} i_A = \{[a,0] \in Z \mid a \in A\}$, e dunque gli elementi in $\operatorname{Coker} i_A$ possono essere scritti come $[0,b]$, per cui la surgettività è ovvia: $\widetilde{i_B}[b] = [0,b]$. D'altronde se $\widetilde{i_B}([b]) = 0$ allora $[0,b] \in \operatorname{Im} i_A$, cioè esiste a tale che $0 = \varphi(a)$ e $b = -\psi(a)$. Ma allora $b \in \operatorname{Im} \psi$ e dunque $[b] = 0$, per cui $\widetilde{i_B}$ è iniettiva. Per quanto detto sopra questo prova la prima parte della tesi.

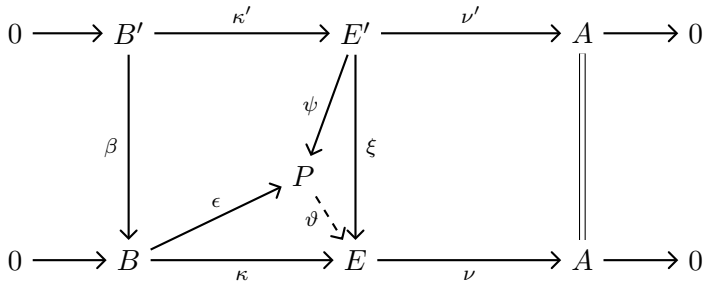
2. Dato che ϑ^{-1} è un isomorfismo e $\alpha = \vartheta^{-1} \circ i_A$ possiamo lavorare direttamente con la costruzione esplicita Z del pushout e mostrare che i_A è iniettiva. Per definizione $i_A(a) = [a,0]$, e per definizione di Z dire $[a,b] = 0$ vuol dire che esiste $x \in X$ tale che $a = \varphi(x)$ e $b = -\psi(x)$. Dunque se a è tale che $i_A(a) = 0$ esiste x tale che $a = \varphi(x)$ e $0 = -\psi(x)$. Per iniettività di ψ allora deve essere $x = 0$, per cui $a = \varphi(x) = \varphi(0) = 0$ e i_A è iniettiva. □

Lemma A.18. Consideriamo il diagramma commutativo con righe esatte

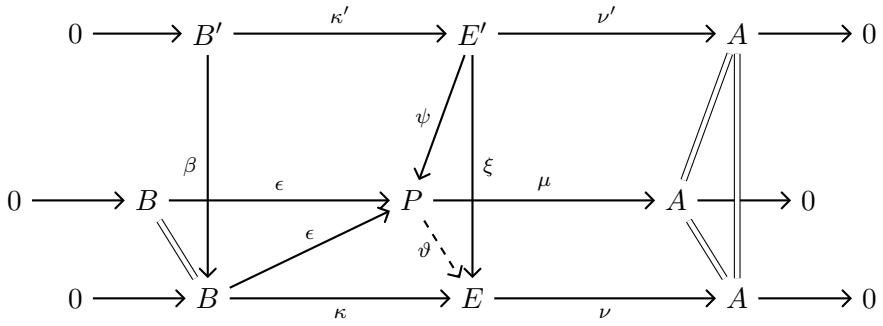
$$\begin{array}{ccccccccc} 0 & \longrightarrow & B' & \xrightarrow{\kappa'} & E' & \xrightarrow{\nu'} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\xi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

allora il quadrato a sinistra è un pushout.

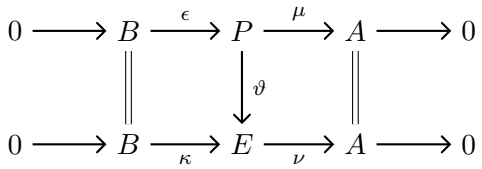
Dimostrazione. Inseriamo un pushout P nel diagramma e consideriamo la ϑ garantita dalla sua proprietà universale:



Chiaramente se mostriamo che ϑ è un isomorfismo abbiamo finito. Per il Lemma precedente[13] ψ induce un isomorfismo fra $\operatorname{Coker}\epsilon$ e $\operatorname{Coker}\kappa'$, che per esattezza è isomorfo ad A, per cui possiamo inserire μ nel diagramma sotto rendendo la riga aggiuntiva esatta e tutti i nuovi quadrati commutativi[14]:



Ora basta cancellare un po' di oggetti e frecce per focalizzare l'attenzione sul diagramma commutativo a righe esatte in basso



e per la Proposizione 6.9 ϑ è un isomorfismo. □

Esercizio A.19. Descrivere le classi di equivalenza di estensioni di $\mathbb{Z}_{12}$ tramite $\mathbb{Z}_{28}$ (mostrando per ciascuna un rappresentante).

Soluzione. Dato che $\operatorname{Ext}^1(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_{\gcd(n,m)}$ e $\gcd(12, 28) = 4$ abbiamo $\operatorname{Ext}^1(\mathbb{Z}_{12}, \mathbb{Z}_{28}) \cong \mathbb{Z}_4$, ed è allora sufficiente trovare quattro estensioni non equivalenti.

Claim: quattro tali estensioni sono (E_i, γ_i, δ_i si intendono come in $0 \to \mathbb{Z}_{28} \xrightarrow{\gamma_i} E_i \xrightarrow{\delta_i} \mathbb{Z}_{12} \to 0$)

0. $E_0 = \mathbb{Z}_{28} \oplus \mathbb{Z}_{12}$, $\gamma_0(a) = (a, 0)$, $\delta_0(a, b) = b$

1. $E_1 = \mathbb{Z}_{336}$, $\gamma_1([n]_{28}) = [12n]_{336}$, $\delta_1([n]_{336}) = [n]_{12}$,

[13] Che è stato enunciato e dimostrato per le frecce verticali, ma ora lo stiamo usando per le frecce orizzontali; chiaramente è solo una questione di come si disegna il diagramma.

[14] I quadrati a sinistra che coinvolgono ϑ commutano per la proprietà di pushout. Verifichiamo che $\nu \circ \vartheta = \mu$. Per ipotesi $\nu \circ \xi = \nu'$ e per la proprietà di pushout $\xi = \vartheta \circ \psi$, per cui $\nu \circ \vartheta \circ \psi = \nu'$. Inoltre $\nu' = \mu \circ \psi$ per definizione di μ, per cui in definitiva abbiamo $\nu \circ \vartheta \circ \psi = \mu \circ \psi$. Ma, come sappiamo dal Lemma precedente, ψ passata al quoziente su $\operatorname{Coker}\kappa' \cong A$ è un isomorfismo, per cui possiamo cancellarla e ottenere $\nu \circ \vartheta = \mu$.

2. $E_2 = \mathbb{Z}_2 \oplus \mathbb{Z}_{168}$, $\gamma_2([1]_{28}) = ([1]_2, [6]_{168})$

$$\delta_2([1]_2, [0]_{168}) = [6]_{12} \qquad \delta_2([0]_2, [1]_{168}) = [1]_{12}$$

3. $E_3 = \mathbb{Z}_{336}$, $\gamma_3([n]_{28}) = [-12n]_{336}$, $\delta_3([n]_{336}) = [n]_{12}$

Il fatto che siano estensioni è una verifica[15]. Se $\{i, j\} \not\subseteq \{1, 3\}$ è palese che E_i ed E_j non sono isomorfi, per cui le rispettive estensioni non possono essere equivalenti; ci basta dunque dimostrare che non esiste nessuna ψ che fa commutare il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_{28} & \xrightarrow{\gamma_1} & E_1 & \xrightarrow{\delta_1} & \mathbb{Z}_{12} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_{28} & \xrightarrow[\gamma_3]{} & E_3 & \xrightarrow[\delta_3]{} & \mathbb{Z}_{12} & \longrightarrow & 0 \end{array}$$

che, scrivendo esplicitamente chi sono E_i, γ_i, δ_i, diventa

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_{28} & \xrightarrow{[n]_{28} \mapsto [12n]_{336}} & \mathbb{Z}_{336} & \xrightarrow{[m]_{336} \mapsto [m]_{12}} & \mathbb{Z}_{12} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_{28} & \xrightarrow[[n]_{28} \mapsto [-12n]_{336}]{} & \mathbb{Z}_{336} & \xrightarrow[[m]_{336} \mapsto [m]_{12}]{} & \mathbb{Z}_{12} & \longrightarrow & 0 \end{array}$$

Se una tale ψ esistesse, per far commutare il rettangolo a destra dovrebbe soddisfare $[\psi([1]_{336})]_{12} = [1]_{12}$, per cui deve essere $\psi([1]_{336}) = [1 + 12k]_{336}$, per un certo $k \in \{0, \ldots, 27\}$, mentre per far commutare il rettangolo a sinistra dovrebbe essere $\psi([12]_{336}) = [-12]_{336}$. In definitiva dovremmo trovare un k tale che $24 + 144k \equiv 0 \pmod{336}$, cioè $24(1 + 6k) \equiv 0 \pmod{336}$. Dato che $2^4 \mid 336$ questo è impossibile: $24 = 2^3 \cdot 3$ e $1 + 6k$ è sempre dispari. □

A.2 A.A. 2013/2014

Alcuni di questi esercizi sono stati risolti in classe durante l'A.A. 2014/2015.

Esercizio A.20. Dato un campo $\mathbb{K}$, si consideri la sottoalgebra $\mathbb{K}[a, b]$ di $\mathbb{K}[X]$, dove $a = X^2$ e $b = X^3$. Dimostrare che gli ideali primi non nulli di $\mathbb{K}[a, b]$ hanno altezza 1.

Soluzione. Si veda l'Esercizio 2.14. □

[15] La verifica meno ovvia, cioè che $\operatorname{Ker} \delta_2 \subseteq \operatorname{Im} \gamma_2$ si fa per casi. Supponiamo che valga $\delta_2([a]_2, [b]_{168}) = [0]_{12}$; allora possono presentarsi due situazioni:

a pari: In questo caso deve essere $b = 12k$, con $k \in \{0, \ldots, 13\}$ e $\gamma_2(2k) = ([a]_2, [b]_{168})$

a dispari: Allora deve essere $b = 6(2k + 1)$, con k come prima, e $\gamma_2(2k + 1) = ([a]_2, [b]_{168})$

Esercizio A.21. Sia $\mathbb{K}$ un campo. Dimostrare che $R = \mathbb{K}[X,Y]/(Y^3 - X^5)$ è un dominio e descrivere la sua chiusura integrale (nel suo campo delle frazioni).

Soluzione. Si veda l'Esercizio 2.15 □

Esercizio A.22. Ricostruire la dimostrazione del teorema che descrive la chiusura integrale $\mathbb{Z}_{(d)}$ di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, a seconda dei casi $d \equiv 1, 2, 3 \pmod 4$, sulla base della traccia data in classe.

Soluzione. Si veda la Sezione 1.3. □

Esercizio A.23. Dimostrare che se d è un intero libero da quadrati tale che $d < -7$ e $d \equiv 1 \pmod 8$ allora la chiusura integrale $\mathbb{Z}_{(d)}$ di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ non è un anello a ideali principali.

Soluzione. Si veda l'Esercizio 1.26. □

Esercizio A.24. Calcolare la dimensione (di Krull) dell'anello $\mathbb{K}[X,Y,Z]/I$ dove $\mathbb{K}$ è un campo e $I = (XY, XZ)$.

Esercizio A.25. Sia R un anello di dimensione di Krull finita d.
a) Dimostrare che, dato un ideale primo $\mathfrak{p}$ in R, non può accadere che esistano tre ideali primi $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{q}_3$ in $R[X]$ la cui contrazione sia uguale a $\mathfrak{p}$.
b) Dimostrare che la dimensione di Krull di $R[X]$ è $\leq 2d + 1$.

Soluzione. Si veda l'Esercizio 5.30. □

Esercizio A.26. Sia A una $\mathbb{K}$-algebra tale che $1 \leq \dim_{\mathbb{K}} A < \infty$ ($\dim_{\mathbb{K}} A$ è la dimensione di A come spazio vettoriale su $\mathbb{K}$).
a) A è artiniana?
b) Supponiamo che A sia locale, con ideale massimale $\mathfrak{m}$. Dimostrare che $\mathfrak{m}^{\dim_{\mathbb{K}} A} = 0$ e dare un esempio in cui $\dim_{\mathbb{K}} A \geq 2$ e $\mathfrak{m}^{\dim_{\mathbb{K}} A - 1} \neq 0$.

Esercizio A.27. Si consideri un sottogruppo finitamente generato G di $GL(n, \mathbb{C})$. Dimostrare che G è residualmente finito, ossia per ogni $g \neq 1$, $g \in G$, esiste un omomorfismo φ_g da G in un gruppo finito tale che $\varphi_g(g) \neq 1$. Questo equivale a dire che esiste un sottogruppo normale di indice finito di G che non contiene g. [Ripensare alla dimostrazione del Lemma di Selberg]

Soluzione. Si veda il Teorema 1.47. □

Esercizio A.28. Sia R un anello e I un ideale. Consideriamo la filtrazione $\{I^n\}$ di R e definiamo la funzione $d\colon R \times R \to \mathbb{Q}^{\geq 0}$ definita così: $d(x,y) = \frac{1}{n+1}$ se $x - y \in I^n \setminus I^{n+1}$, $d(x,y) = 0$ altrimenti. Dimostrare che d è simmetrica e soddisfa la disuguaglianza triangolare. Sotto quale ulteriore condizione d è una metrica?

Esercizio A.29. Sia $\varphi\colon \widehat{\mathbb{Z}}_{(10)} \to \widehat{\mathbb{Z}}_{(2)} \oplus \widehat{\mathbb{Z}}_{(5)}$ l'isomorfismo standard. Trovare $w \in \widehat{\mathbb{Z}}_{(10)}$ tale che $\varphi(w) = (0, 1)$.

Soluzione. Si veda l'Esercizio 4.10. □

Esercizio A.30. Sia R un anello e I un ideale. È vero o falso che $\widehat{R}_I$ dominio implica R dominio?

Soluzione. Si veda l'Esercizio A.9. □

Esercizio A.31. Sia p un numero primo, e siano $A = \bigoplus_{n=1}^{\infty} \mathbb{Z}_p$ e $B = \bigoplus_{n=1}^{\infty} \mathbb{Z}_{p^n}$. Si consideri l'omomorfismo di $\mathbb{Z}$ moduli $\alpha\colon A \to B$ che, componente per componente, è dato dalla immersione ovvia $\mathbb{Z}_p \to \mathbb{Z}_{p^n}$; a questo punto A può essere visto come sottomodulo di B. Dimostrare che il (p) completamento di A non è isomorfo al completamento di A indotto dal (p) completamento di B (quindi non vale Artin-Rees).

Soluzione. Si veda il Controesempio 4.31. □

Esercizio A.32. Sia R un anello noetheriano e I un ideale. Dimostrare il teorema di intersezione di Krull (esiste $r \in I$ tale che $(1 - r) \bigcap I^n = 0$) nel modo indicato dai passi seguenti:
a) Osservare che basta dimostrare che per ogni $x \in \bigcap I^n$ vale $x \in xI$.
b) Sia $I = (a_1, a_2, \ldots, a_s)$ e sia $x \in \bigcap I^n$. Osservare che per ogni $n \geq 1$ esiste un polinomio omogeneo di grado n $P_n(X_1, X_2, \ldots, X_s)$ in $R[X_1, X_2, \ldots, X_s]$ tale che $x = P_n(a_1, a_2, \ldots, a_s)$.
c) Considerare gli ideali $J_n = (P_1, \ldots, P_n)$ in $R[X_1, X_2, \ldots, X_s]$. Osservare che, preso $N \in \mathbb{N}$ tale che la successione dei J_n si stabilizza da J_N in poi, si può scrivere:

$$P_{N+1} = \sum_{i=1}^{N} Q_{N-i+1} P_i$$

per certi polinomi *omogenei* Q_i (di grado $i > 0$) in $R[X_1, X_2, \ldots, X_s]$.
d) Concludere che $x \in xI$.

Soluzione. Si veda alla fine della Sezione 4.2. □

Esercizio A.33. Sia A un anello locale con ideale massimale $\mathfrak{m}$, completo rispetto alla topologia $\mathfrak{m}$-adica. Si consideri il gruppo moltiplicativo

$$U = \{1 + a \mid a \in \mathfrak{m}\}$$

e sia n un intero positivo che non è diviso dalla caratteristica di $A/\mathfrak{m}$. Dimostrare che la mappa $\varphi\colon U \to U$ definita da $\varphi(x) = x^n$ è un automorfismo del gruppo U.

Soluzione. Si veda l'Esercizio 4.39. □

Esercizio A.34. Sia R un anello e $I \subset R$ un ideale. Siano M, N due R moduli con I filtrazioni

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

$$N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \dots$$

Sia $f\colon M \to N$ un omomorfismo che rispetta le filtrazioni, ossia $f(M_i) \subseteq N_i$ per ogni i e sia $\mathrm{gr}(f)$ il corrispondente omomorfismo fra i moduli graduati $\mathrm{gr}(M)$ e $\mathrm{gr}(N)$. Supponiamo inoltre che $\cap M_r = \{0\}$.
a) È vero o falso che f iniettivo implica $\mathrm{gr}(f)$ iniettivo?
b) È vero o falso che $\mathrm{gr}(f)$ iniettivo implica f iniettivo?

Esercizio A.35. Sia $\mathbb{K}$ un campo di caratteristica 0 e sia R il dominio locale $\mathbb{K}[X,Y]_{(X,Y)}$. Sia $g = Y^2 - X^2(X+1)$ in R. Dimostrare che il quoziente $S = R/gR$ è un dominio locale. Sia $\mathfrak{m}$ il suo ideale massimale. Dimostrare che $\widehat{S}_{\mathfrak{m}}$ non è un dominio.

Esercizio A.36. Descrivere le classe di equivalenza di estensioni di $\mathbb{Z}_{12}$ tramite $\mathbb{Z}_{28}$ (mostrando per ciascuna un rappresentante).

Soluzione. Si veda l'Esercizio A.19. □

Esercizio A.37. Si consideri l'ideale $\mathfrak{p} = (7, X, Y, Z)$ in $A = \mathbb{Z}[X,Y,Z]$ e sia B il quoziente di $A_{\mathfrak{p}}$ per l'ideale generato da $Z^2 - X^3 - X - Y^2$. Calcolare la dimensione di B e dire se è regolare.

Soluzione. Si veda l'Esercizio 5.28. □

Esercizio A.38. Dato l'anello $A = \mathbb{Z}[X,Y]$ consideriamo l'ideale $I = (X^2 - XY + X, XY - Y^2 + Y)$. Calcolare la dimensione di $B = A/I$.

Soluzione. Si veda l'Esercizio 5.35. □

Esercizio A.39. Dimostrare la seguente generalizzazione del "lemma di evitamento".

Sia A un anello, e siano $P_1, P_2, \dots, P_k$, con $k \geq 2$, degli ideali di cui almeno $k-2$ siano primi. Dato un ideale I, se $I \subseteq P_1 \cup P_2 \cup \dots \cup P_k$ allora esiste un indice i per cui $I \subseteq P_i$.

[Suggerimento, da ritenersi parte del testo. Per induzione su k. Nel passo induttivo, supponiamo la proposizione vera fino a $k-1$ e supponiamo di sapere che per ogni $i \geq 3$ P_i è primo. Sia $I \subseteq P_1 \cup P_2 \cup \dots \cup P_k$. Se ci sono relazioni di inclusione fra i P_i ne possiamo eliminare qualcuno e applichiamo l'ipotesi induttiva. Supponiamo dunque che fra i P_i non ci siano inclusioni. Se $I \subseteq P_1 \cup P_2 \cup \dots \cup P_{k-1}$ si applica l'ipotesi induttiva, altrimenti dobbiamo mostrare che $I \subseteq P_k$. Prendiamo un elemento $s_j \in P_j \setminus P_k$ per ogni $j \leq k-1$ e sia $s = s_1 s_2 \cdots s_{k-1}$. Preso un elemento $x \in I$, vogliamo mostrare che $x \in P_k$. Costruiamo l'elemento $z = sx + y$, dove y lo scegliamo in $I \setminus P_1 \cup P_2 \cup \dots \cup P_{k-1} \dots$]

Esercizio A.40. Sia A un dominio noetheriano. Dimostrare che i seguenti due fatti sono equivalenti:
a) Esiste un $f \in A \setminus \{0\}$ tale che A_f è un campo.
b) A ha un numero finito di ideali massimali e ha dimensione ≤ 1.

Esercizio A.41. a) Siano I e J due ideali di un anello R. Dimostrare che c'è una successione esatta

$$0 \to (I \cap J)/IJ \to I \otimes_R (R/J) \to R/J \to (R/I) \otimes_R (R/J) \to 0$$

b) Dare un esempio di un anello R e un ideale I tali che la proiezione $R \to R/I$ non sia una mappa piatta.

Esercizio A.42. Sia R un anello e siano

$$0 \to A \to P \xrightarrow{\varphi} B \to 0$$

$$0 \to A' \to P' \xrightarrow{\varphi'} B \to 0$$

due successioni esatte di R moduli, dove P e P' sono proiettivi. Dimostrare che gli R moduli $A \oplus P'$ e $A' \oplus P$ sono isomorfi.

[Costruire $X = \{(p, q) \in P \oplus P' \mid \varphi(p) = \varphi'(q)\}$ (si tratta del pullback di $P \xrightarrow{\varphi} B$ e $P' \xrightarrow{\varphi'} B$) e considerare la proiezione $\pi \colon X \to P \dots$]

Esercizio A.43. Dati gli $\mathbb{Z}$-moduli $\mathbb{Z}_{36}$ e $\mathbb{Z}_{42}$, calcolare il gruppo abeliano $\mathrm{Ext}(\mathbb{Z}_{36}, \mathbb{Z}_{42})$. Descrivere (mostrando un rappresentante) almeno una classe di equivalenza di estensioni di $\mathbb{Z}_{36}$ tramite $\mathbb{Z}_{42}$ che non corrisponda a $0 \in \mathrm{Ext}(\mathbb{Z}_{36}, \mathbb{Z}_{42})$.

Soluzione. Si veda l'Esercizio 7.36. □

Appendice B

Un Po' di Geometria

Durante il corso il prof. Frigerio ha tenuto un seminario di un'ora su un'interazione di geometria ed algebra di cui è responsabile il Teorema di Residuale Finitezza. Questa appendice è (il risultato di) un tentativo di prendere appunti, e non fa parte del programma del corso ai fini dell'esame per l'A.A. 2014/2015. Il Lemma di Selberg a quanto pare è fondamentale nella teoria degli *orbifold*, ma parlarne richiede troppi prerequisiti.

Vogliamo dimostrare questo fatto:

Teorema B.1. Il gruppo libero su n generatori F_n è residualmente finito.

Dato che sappiamo che i gruppi lineari finitamente generati sono residualmente finiti l'idea è realizzare F_n come gruppo di matrici. Vedremo prima il caso F_2, che realizzeremo come sottogruppo di $\mathrm{SL}_2(\mathbb{R})$, e poi generalizzeremo al caso $n > 2$. Ci serve il seguente risultato molto usato nella Teoria Geometrica dei Gruppi:

Lemma B.2 (del Ping-Pong)**.** Sia $G = \langle a, b \rangle$, che agisce su un insieme X, e si supponga che[1]

1. a e b abbiano ordine infinito
2. esistano $X_1, X_2 \subseteq X$ disgiunti tali che per ogni $m \neq 0$ si abbia $a^m(X_1) \subseteq X_2$ e $b^m(X_2) \subseteq X_1$.

Allora G è libero con generatori a e b.

L'idea è che prese due matrici a caso è facile che generino un gruppo libero; tuttavia prese due matrici in particolare mostrare che effettivamente non soddisfano alcuna relazione non è esattamente una fesseria, perlomeno detto così. Vediamo la dimostrazione del Lemma (che chiarirà anche il perché del nome).

[1] La prima ipotesi è in realtà superflua perché segue dalla seconda.

Dimostrazione. Sia $w = a^{n_1}b^{m_1}a^{n_2}b^{m_2}\dots a^{n_k}$ una parola ridotta, cioè con gli $n_i, m_i \neq 0$ e senza cancellazioni formali[2]. Trattiamo prima questo caso e poi vediamo che ci si può ricondurre. Se $g \in G$ è l'elemento determinato da w abbiamo, usando la seconda ipotesi

$$g(X_1) = a^{n_1}b^{m_1}a^{n_2}b^{m_2}\dots a^{n_k}(X_1) \subseteq X_2$$

e dato che $X_1 \cap X_2 = \emptyset$ abbiamo $g \neq 1$. Vediamo come trattare tutte le altre parole, che possiamo senza alcun problema supporre ridotte. In questo caso esiste $m \ggg 0$ tale che $a^m w a^{-m}$ è della forma già analizzata (una volta ridotta). Questo conclude perché se in G vale $a^m w a^{-m} \neq 1$, chiaramente non può essere $w = 1$. □

Teorema B.3. $\langle a, b\rangle = F_2 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ tramite[3]

$$a \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad b \mapsto \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Dimostrazione. Sia $X = \mathbb{R}^2$ e poniamo

$$X_1 = \{(x, y) \in \mathbb{R}^2 \mid |x| < |y|\} \qquad X_2 = \{(x, y) \in \mathbb{R}^2 \mid |x| > |y|\}$$

Abbiamo

$$a^m = \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \qquad b^m = \begin{pmatrix} 1 & 0 \\ 2m & 1 \end{pmatrix} \qquad a^m \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2my \\ y \end{pmatrix}$$

Se $|y| > |x|$ e $m \neq 0$ abbiamo $|x + 2my| > |y|$, e quindi $a^m(X_1) \subseteq X_2$ se $m \neq 0$. Analogamente per $|x| > |y|$ e per b. □

Questo mostra che F_2 è residualmente finito. Inoltre la proprietà di residuale finitezza passa in maniera ovvia ai sottogruppi, e si può mostrare che

Teorema B.4. F_n è un sottogruppo di F_2.

Prima di dimostrarlo notiamo che

Osservazione B.5. Se G è residualmente finito e $S \subseteq G \setminus \{1\}$ è finito allora esiste $f\colon G \to F$ gruppo finito tale che $\forall g \in S\ f(g) \neq 1$: basta invocare la residuale finitezza di G su ogni $s \in S$ ottenendo F_s e φ_s, poi porre $F = \bigoplus_{s\in S} F_s$ e definire $f\colon G \to F$ come $\bigoplus_{s\in S} \varphi_s$.

Definizione B.6. Un grafo per noi è un grafo finito e connesso, eventualmente con archi multipli fra due vertici e con archi anche da un vertice a sé stesso, metrizzato assegnando ad ogni lato lunghezza 1 e munito della topologia indotta. Possiamo pensarlo come CW-complesso.

[2] Per capirci, che non contiene cose del tipo aa^{-1}. In questo caso, per le ipotesi su a e b, è ovvio.

[3] "Dimostrare questa cosa direttamente non è... sicuramente non è sano."

Teorema B.7. Sia Γ un grafo con v vertici ed e lati. Allora $\pi_1(\Gamma) = F_{1+e-v}$.

Dimostrazione. L'idea è che ogni arco con estremi distinti può essere collassato tramite equivalenza omotopica preservando sia il π_1 che $1 + e - v$ (stiamo togliendo sia un arco che un vertice) e ottenendo un bouquet di S^1. Questo ha un solo vertice, per cui $1 + e - v = e$, ed ha $\pi_1 = F_e$ per Van Kampen. □

Ora sappiamo che se Γ è un grafo esiste una bigezione fra i sottogruppi di $\pi_1(\Gamma)$ e i rivestimenti di Γ modulo isomorfismo che associa sottogruppi di indice d a rivestimenti di grado d, modulo autismi, puntatura, e tecnicaglie varie che vivono nel corso di Geometria 2.

Dimostrazione del Teorema B.4. Sia $n > 2$ e scegliamo $d \ggg 1$. Esiste un mappa surgettiva (abelianizzazione) $F_2 \twoheadrightarrow \mathbb{Z}^2$. Componiamola con un'altra mappa surgettiva

$$F_2 \twoheadrightarrow \mathbb{Z}^2 \twoheadrightarrow \mathbb{Z}_d$$

ottenendo una mappa il cui nucleo K ha indice d in F_2. Sia Γ il bouquet di due S^1 e $\tilde{\Gamma}$ il rivestimento di grado d associato a K, che ha $dv(\Gamma)$ vertici e $de(\Gamma)$ archi, e quindi il suo π_1 è $F_{1+2d-d} = F_{1+d}$. Abbiamo quindi realizzato F_{1+d} come sottogruppo di F_2. □

Corollario B.8. $\forall n \geq 2$ F_n è residualmente finito.

Definizione B.9. Un *ciclo* in un grafo è un loop iniettivo.

Teorema B.10. Siano Γ un grafo (finito) ed $R \geq 0$. Allora esiste $\tilde{\Gamma}$ rivestimento finito di Γ tale che ogni ciclo di $\tilde{\Gamma}$ ha lunghezza $\geq R$.

Dimostrazione. Tempo scaduto. L'idea è che il numero di loop (anche non iniettivi, ma localmente iniettivi) di lunghezza $\leq R$ in Γ è finito (a meno di riparametrizzazioni). Questi cammini identificano un sottoinsieme finito di $\pi_1(\Gamma) \setminus \{\mathrm{id}\}$ e abbiamo un sottogruppo di indice finito che li evita tutti per l'Osservazione B.5. Il rivestimento associato a questo sottogruppo funziona. □

Appendice C

Metodi Omologici in Algebra Commutativa

Il contenuto di questa appendice è ricavato da una lezione del prof. Maffei ed è, almeno per l'A.A. 2014/2015, facoltativo ai fini dell'esame.

Come abbiamo visto, quando si ha a che fare con funtori derivati è importante scegliere una risoluzione proiettiva/libera di un oggetto dato in maniera furba: più la risoluzione è "bella" (che tipicamente vuol dire "corta") più è facile fare i conti. In qualche caso questa idea può essere sviscerata:

Definizione C.1. Se $(A, \mathfrak{m})$ è un anello locale noetheriano, una risoluzione libera di un A-modulo M finitamente generato

$$\cdots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \to 0$$

si dice *minimale* se $F_i \cong A^{b_i}$, con b_0 il minimo numero di generatori di M e, per $i \geq 1$, b_i il minimo numero di generatori di $\operatorname{Ker} \delta_{i-1}$.

Chiaramente la definizione ha senso vista la noetherianità di A e la finita generatezza di M. L'idea è quindi che una risoluzione minimale si costruisce "economizzando" sul numero di generatori ogni volta che costruiamo un nuovo F_i; fra qualche pagina mostreremo che una "risoluzione minimale" è *veramente* minimale, nel senso che non ce ne sono di più corte.

Lemma C.2. Sia A locale noetheriano e M finitamente generato. Se pensiamo $\mathbb{K} = A/\mathfrak{m}$ come A-modulo, una risoluzione libera

$$\cdots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \to 0$$

è minimale se e solo se per ogni $i \geq 1$ la mappa

$$\bar{\delta}_i \colon F_i \otimes_A \mathbb{K} \to F_{i-1} \otimes_A \mathbb{K}$$

è nulla.

Prima di dimostrare il Lemma ricordiamo che

Osservazione C.3. $N \otimes_A \mathbb{K} = N \otimes_A A/\mathfrak{m} \cong N/\mathfrak{m}N$, per cui dire che le $\bar{\delta}_i$ sono nulle è equivalente a chiedere che $\operatorname{Im} \delta_i \subseteq \mathfrak{m}F_{i-1}$.

Nella dimostrazione faremo uso estensivo del seguente

Fatto C.4. Se N è finitamente generato, il minimo numero a di generatori di N è uguale a $b = \dim_{\mathbb{K}} N/\mathfrak{m}N = \dim_{\mathbb{K}} N \otimes_A \mathbb{K}$.

Dimostrazione del Fatto. La disuguaglianza $a \geq b$ è ovvia, e per Nakayama[1] i generatori di $N/\mathfrak{m}N$ si sollevano, per cui $a \leq b$. □

Dimostrazione del Lemma. Mostriamo il "⇒". Dato che $- \otimes_A \mathbb{K}$ è esatto a destra tensorizzando la risoluzione troviamo la successione esatta

$$F_1 \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_1} F_0 \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_0} M/\mathfrak{m}M \to 0$$

Per definizione di risoluzione minimale sia $F_0 \otimes_A \mathbb{K}$ che $M/\mathfrak{m}M$ sono isomorfi a $\mathbb{K}^{b_0}$. Dato che per esattezza $\bar{\delta}_0$ è surgettiva, e che è una mappa fra spazi vettoriali[2] della stessa — finita — dimensione, è anche iniettiva, dunque

$$0 = \operatorname{Ker} \bar{\delta}_0 = \operatorname{Im} \bar{\delta}_1$$

e quindi $\bar{\delta}_1 = 0$. Per $i > 1$, consideriamo

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{\delta_{i+1}} & F_i & \xrightarrow{\delta_i} & F_{i-1} & \xrightarrow{\delta_{i-1}} & F_{i-2} & \xrightarrow{\delta_{i-2}} & \cdots \\ & & & & & \searrow \quad \nearrow & & & \\ & & & & & \widetilde{M} & & & \\ & & & & & \nearrow \quad \searrow & & & \\ & & & & 0 & & 0 & & \end{array}$$

Guardiamo la successione "storta" che finisce su $\widetilde{M} \to 0$, tensorizziamola e per comodità grafica raddrizziamola:

$$F_i \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_i} F_{i-1} \otimes_A \mathbb{K} \xrightarrow{\pi} \widetilde{M}/\mathfrak{m}\widetilde{M} \to 0$$

A questo punto dovrebbe essere chiaro che lo stesso ragionamento di prima conclude: dato che per ipotesi $\widetilde{M} \cong \operatorname{Ker} \delta_{i-2}$ ha come minimo numero di generatori b_{i-1} e che $F_{i-1} \cong A^{b_{i-1}}$, la mappa

$$\pi \colon F_{i-1} \otimes_A \mathbb{K} \to \widetilde{M} \otimes_A \mathbb{K}$$

è surgettiva fra $\mathbb{K}$-spazi vettoriali di dimensione b_{i-1}, quindi è iniettiva, e per esattezza $\bar{\delta}_i$ è la mappa nulla.

[1] Vedi Proposizione 2.8 in [2].

[2] Il prodotto tensore induce una struttura di $\mathbb{K}$-modulo, cioè di $\mathbb{K}$-spazio vettoriale. Vedi [2], subito dopo la Proposizione 2.16.

Mostriamo il "$\Leftarrow$". Per $i = 0$ basta notare che la successione

$$F_1 \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_1} F_0 \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_0} M \otimes_A \mathbb{K} \to 0$$

è esatta, e per ipotesi $\bar{\delta}_1 = 0$, per cui è esatta anche

$$0 \to F_0 \otimes_A \mathbb{K} \xrightarrow{\bar{\delta}_0} M \otimes_A \mathbb{K} \to 0$$

dunque $\bar{\delta}_0$ è un isomorfismo, e $\dim_{\mathbb{K}} F_0 \otimes_A \mathbb{K} = \dim_{\mathbb{K}} M \otimes_A \mathbb{K}$ che, in combinazione con il Fatto C.4, è la tesi. Il caso $i > 0$ segue come prima "spezzando" la risoluzione. □

Definizione C.5. Se $(A, \mathfrak{m})$ è locale noetheriano ed M è finitamente generato, la sua *dimensione proiettiva* $\mathrm{pd}(M)$ è il minimo n tale che esiste una sua risoluzione proiettiva lunga n (nel senso che il modulo più a sinistra non nullo è P_n) o $+\infty$ se non ne esistono di lunghezza finita.

Osservazione C.6. Se F è un funtore additivo e calcoliamo il funtore derivato $L_iF(M)$, per $i > \mathrm{pd}(M)$ questo è nullo.

Dimostrazione. Se abbiamo una risoluzione

$$\cdots \to 0 \to 0 \to P_a \to \cdots \to P_0 \to M \to 0$$

e la usiamo per calcolare L_iF

$$\cdots \to 0 \to 0 \to FP_a \to \cdots \to FP_0 \to 0$$

otteniamo subito che i L_iF sono nulli per $i > a$. □

Definizione C.7. La *dimensione globale* di A è

$$\text{gl-dim}(A) = \sup\{\mathrm{pd}(M) \mid M \text{ finitamente generato}\}$$

Spoiler C.8. Se A è locale regolare questa dimensione coincide con quelle che conosciamo, altrimenti è $+\infty$.

Teorema C.9. Sia $(A, \mathfrak{m})$ locale noetheriano, M un A-modulo finitamente generato, $\mathbb{K} = A/\mathfrak{m}$ il suo campo residuo e poniamo

$d =$ $\mathrm{pd}(M)$

$\ell =$ la lunghezza di una[3] risoluzione libera minimale $\{F_i\}$ di M,

$t =$ $\min\{j \mid \forall i > j \ \mathrm{Tor}_i(\mathbb{K}, M) = 0\}$

Allora $d = \ell = t$. Inoltre, posto $F_i \cong A^{b_i}$, si ha $b_i = \dim_{\mathbb{K}} \mathrm{Tor}_i(\mathbb{K}, M)$.

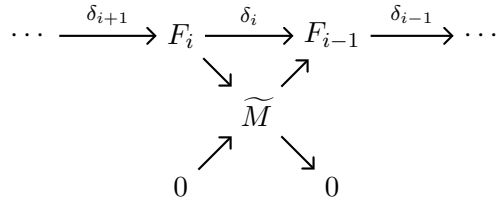
[3]Per ora intendiamo la risoluzione fissata a monte ma, come conseguenza del Teorema, tutte le risoluzioni libere minimali avranno la stessa lunghezza.

La seconda parte dell'enunciato ha senso perché i $\mathbb{K} \otimes_A F_i$ sono $\mathbb{K}$-spazi vettoriali, e quindi lo sono anche[4] i $\operatorname{Tor}_i(\mathbb{K}, M)$. Inoltre segue immediatamente dal Teorema che, come anticipato, una risoluzione minimale ha lunghezza minima: se ci fosse una risoluzione (anche non minimale) di lunghezza $a < \ell$ la serie di Tor_i nulli comincerebbe prima e avremmo $t \leq a < \ell = t$.

Dimostrazione. Alcune disuguaglianze sono ovvie: $\ell \geq d \geq t$. Infatti $\ell \geq d$ perché ogni risoluzione libera è una risoluzione proiettiva, e $d \geq t$ per l'Osservazione C.6. Se ora prendiamo una risoluzione minimale[5]

$$0 \to F_\ell \to \cdots \to F_1 \to F_0 \to M \to 0$$

e mostriamo che per $0 \leq i \leq \ell$ vale $\operatorname{Tor}_i(\mathbb{K}, M) \cong \mathbb{K}^{b_i}$ abbiamo simultaneamente sia $t \geq \ell$ che la seconda parte del Teorema[6]. Per $i = 0$ è vero: $\operatorname{Tor}_0(\mathbb{K}, M) = \mathbb{K} \otimes_A M$ e per definizione (usando il Fatto C.4) b_0 è la sua dimensione. Per $i > 0$ spezziamo



Da una parte, tramite un'argomentazione che a questo punto dovrebbe essere diventata routine, $\dim_{\mathbb{K}} \widetilde{M} \otimes_A \mathbb{K} = b_i$. D'altra parte per il Lemma C.2 abbiamo $\bar{\delta}_i = 0$, per cui guardando il complesso

$$\cdots \to 0 \to F_\ell \otimes_A \mathbb{K} \xrightarrow{0} F_{\ell-1} \otimes_A \mathbb{K} \xrightarrow{0} \cdots \xrightarrow{0} F_0 \otimes_A \mathbb{K} \to 0$$

abbiamo subito, per $i \leq \ell$,

$$\operatorname{Tor}_i(\mathbb{K}, M) = H_i(\{F_j\} \otimes_A \mathbb{K}) \cong \frac{\operatorname{Ker} \bar{\delta}_i}{\operatorname{Im} \bar{\delta}_{i-1}} \cong \frac{F_i \otimes_A \mathbb{K}}{0} \cong \mathbb{K}^{b_i} \qquad \square$$

Quanto visto finora vale anche se invece di un anello locale consideriamo l'anello graduato $A = \mathbb{K}[t_1, \ldots, t_m]$ e consideriamo solo moduli graduati, morfismi di moduli graduati, risoluzioni graduate, eccetera. Tuttavia per far tornare le cose[7] si "cambia" la definizione di modulo graduato libero dando la possibilità di cambiare il grado ai generatori. Ad esempio $M = A^2$ si può graduare come $M_0 = 0$, $M_1 = A_0 \oplus 0$, $M_i = A_{i-1} \oplus A_{i-2}$. Inoltre bisogna anche "rimpiazzare" Nakayama, nel senso che vorremmo dire che se

[4] Se non è chiaro perché si ripercorrano le definizioni.

[5] Nel senso della Definizione C.1.

[6] Basta rileggere attentamente l'enunciato.

[7] Il punto è che, ad esempio, vogliamo risolvere $A^2 \to (x, y^2) \to 0$, ma questa mappa non ha né grado 1 né 2 se usiamo le gradazioni ovvie.

M è finitamente generato e graduato $\mathfrak{m}M = M$ implica $M = 0$, e questo è chiaramente[8] vero se poniamo $\mathfrak{m} = (t_1, \ldots, t_m)$, dopodiché tutto può essere enunciato pari pari (notare che anche in questo caso $A/\mathfrak{m}$ è un campo: esattamente $\mathbb{K}$). Essenzialmente bisogna scrivere "graduato" ovunque, e funziona tutto perché l'unico risultato dove abbiamo usato la località è quel corollario di Nakayama per sollevare i generatori da $M/\mathfrak{m}M$ a M, ma si rimpiazza con un risultato analogo per i graduati. Ad esempio se $M = M_0 \oplus M_1 \oplus \ldots$, con[9] $M_0 \neq 0$, allora $\mathfrak{m}M = M_1 \oplus M_2 \oplus M_3 \ldots$, e non è difficile sollevare generatori di $M/\mathfrak{m}M$ a generatori di M.

Quello che vediamo ora è essenzialmente considerato (in retrospettiva) il primo Teorema di algebra omologica. Ci mettiamo nel caso graduato, e del caso locale regolare parleremo dopo.

Teorema C.10 (delle Sizigie di Hilbert)**.** Sia $A = \mathbb{K}[t_1, \ldots, t_n]$. Allora se B è un A-modulo graduato finitamente generato, B ha una risoluzione libera graduata di lunghezza n.

Dimostrazione. Poniamo $\mathfrak{m} = (t_1, \ldots, t_n)$ e consideriamo $\mathbb{K} \cong A/\mathfrak{m}$ come A-modulo[10]. Vogliamo mostrare che $\operatorname{Tor}_i(\mathbb{K}, B) = 0$ per $i > n$, che per la versione graduata del Teorema C.9 è equivalente alla tesi. Per fare questo possiamo sia risolvere B che risolvere $\mathbb{K}$; il trucco è proprio optare per la seconda ipotesi. Vediamo quella che si chiama[11] *risoluzione di Koszul* di $\mathbb{K}$. Questa è una risoluzione in A-moduli graduati liberi costruita come segue. Poniamo $M = A^n$ e definiamo[12]

$$t = (t_1, \ldots, t_n) = t_1 e_1 + \ldots + t_n e_n \in A^n = M$$

dove $\{e_i\}$ è la base standard di $M = A^n$. Indicando con $\bigwedge^i M$ l'i-esimo prodotto esterno definiamo $K_\bullet$ come[13]

$$0 \to \underbrace{\bigwedge^0 M}_{=A=F_n} \xrightarrow{\partial_n = t\wedge -} \underbrace{\bigwedge^1 M}_{=M=F_{n-1}} \xrightarrow{\partial_{n-1} = t\wedge -} \underbrace{\bigwedge^2 M}_{=F_{n-2}} \xrightarrow{\partial_{n-2} = t\wedge -} \cdots \xrightarrow{t\wedge -} \underbrace{\bigwedge^n M}_{=F_0 \simeq A}$$

Questo $K_\bullet$ è un complesso perché $t \wedge t = 0$. Inoltre F_i è libero[14], e $\delta_i(F_i) \subset \mathfrak{m}F_{i-1}$, perché $t \wedge v = \sum t_i(e_i \wedge v)$. Ne segue che, se mostriamo che $K_\bullet$ è una risoluzione di $\mathbb{K}$, allora sarà minimale per il Lemma C.2 e l'Osservazione C.3.

Se ora mostriamo che $K_\bullet$ è effettivamente una risoluzione di $\mathbb{K}$ abbiamo finito: abbiamo fra le mani una risoluzione minimale di $\mathbb{K}$ lunga n e quindi

[8] Moltiplicare per elementi di $\mathfrak{m}$ aumenta il grado, quindi se $M = \mathfrak{m}M \ldots$

[9] Wlog, sennò sarà, boh, M_5.

[10] Dunque l'azione è "valutare i polinomi in 0".

[11] O forse "somiglia alla".

[12] Notazione infelice: occhio a non confondere la n-upla $(t_1, \ldots, t_n)$ con l'ideale $\mathfrak{m}$.

[13] Chiaramente si intende che a sinistra continui con tutti 0: ci avrei inserito dei puntini e una freccia ma poi non ci stava tutto in una riga.

[14] È isomorfo ad $A^{\binom{n}{i}}$.

per l'Osservazione C.6 $\mathrm{Tor}_i(\mathbb{K}, N) = 0$ per ogni $i > n$ e per ogni N, e in particolare per B. La dimostrazione è quindi conclusa a patto di dimostrare il prossimo Lemma. □

Lemma C.11. Se $1 \leq i \leq n$, allora $H_i(K_\bullet) = 0$, mentre $H_0(K_\bullet) \simeq \mathbb{K}$.

Dimostrazione del Lemma. Per $r \leq n$ definiamo $M_r = A^r$ e introduciamo un nuovo complesso $K^r_\bullet$ definito come

$$\cdots \to 0 \to \bigwedge^0 M_r \xrightarrow{x_r \wedge -} \bigwedge^1 M_r \xrightarrow{x_r \wedge -} \cdots \xrightarrow{x_r \wedge -} \bigwedge^r M_r \to 0$$

dove $x_r = t_1 e_1 + \ldots + t_r e_r$. Dimostriamo, per induzione su r, che

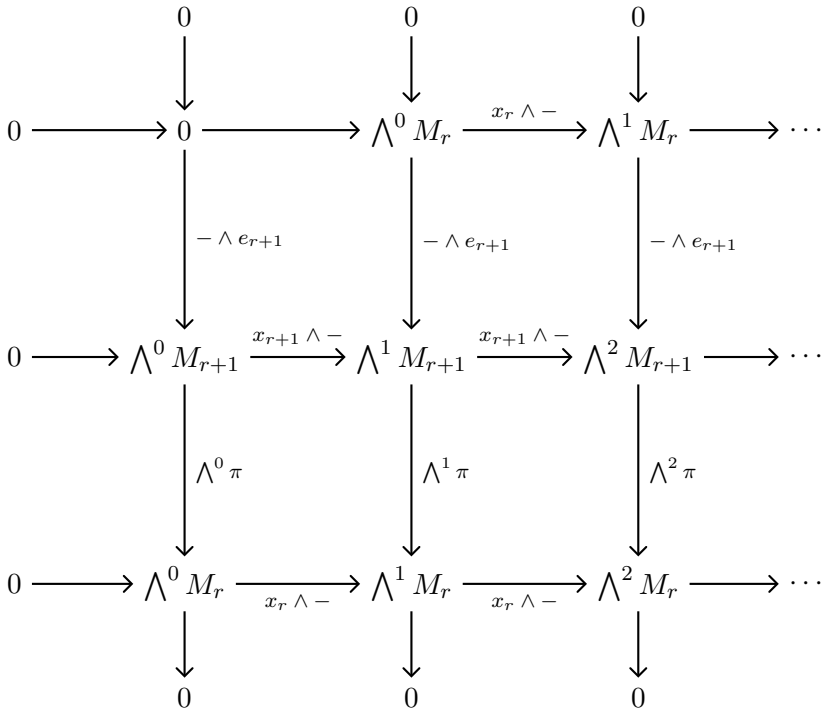
$$\begin{cases} H_0(K^r_\bullet) \cong A/(t_1, \ldots, t_r) \\ H_i(K^r_\bullet) = 0 & \text{per } 1 \leq i \leq r \end{cases}$$

Questo conclude, perché il caso $n = r$ è la tesi.

Per $r = 1$ abbiamo $M_1 = A \cong \bigwedge^0 A \cong \bigwedge^1 A$, e $K^1_\bullet$ è il complesso

$$0 \to A \xrightarrow{\cdot t_1} A \to 0$$

Dato A è un dominio la moltiplicazione per t_1 è iniettiva e si ha subito la tesi. Per il passo induttivo disegniamo il diagramma[15]



[15] L'ultima riga sarebbe più corta delle altre due: ci si aggiunge uno 0 in fondo.

Le mappe $\bigwedge^i \pi$ sono quelle indotte dalla proiezione $\pi\colon M_{r+1} \to M_r$, che quindi mandano in 0 qualunque cosa si possa scrivere come $w \wedge e_{r+1}$ e sono l'identità altrimenti; ne segue che la mappa $\bigwedge^0 \pi$ è iniettiva è surgettiva (di fatto è l'identità). Inoltre $M_{r+1} = M_r \oplus A_{e_{r+1}}$, e in generale

$$\bigwedge^i M_{r+1} \cong \bigwedge^i M_r \oplus \left(\left(\bigwedge^{i-1} M_r \right) \wedge e_{r+1} \right)$$

per cui le colonne sono esatte. Inoltre è possibile mostrare[16] che tutti i quadrati commutano: abbiamo quindi tre complessi e una successione esatta fra loro, e possiamo scrivere la successione esatta lunga in omologia[17]

$$0 \to H_{r+1}(K_\bullet^{r+1}) \to H_r(K_\bullet^r) \to H_r(K_\bullet^r) \to H_r(K_\bullet^{r+1}) \to H_{r-1}(K_\bullet^r) \to \cdots$$

Occhio al quarto termine (da sinistra): è proprio H_r, perché sarebbe H_{r-1} ma la successione della riga più in alto è quella della riga più in basso shiftata (guardare il diagramma!!). Per ipotesi induttiva conosciamo già tutti i termini della successione che non coinvolgono $K_\bullet^{r+1}$, e sappiamo che quelli di indice ≥ 1 sono tutti nulli. Riscriviamo dunque la successione come

$$\begin{aligned} 0 \to H_{r+1}(K_\bullet^{r+1}) \to 0 \to 0 \to H_r(K_\bullet^{r+1}) \to 0 \to \\ \to 0 \to H_{r-1}(K_\bullet^{r+1}) \to 0 \to 0 \to H_{r-2}(K_\bullet^{r+1}) \to 0 \to \cdots \end{aligned}$$

Per esattezza dunque $H_i(K_\bullet^{r+1}) = 0$, almeno per $2 \leq i \leq r+1$ (abbiamo usato che $H_{i-1} = 0$). Vediamo cosa succede alla fine della successione:

$$\cdots \to \underbrace{H_1(K_\bullet^r)}_{=0} \to H_1(K_\bullet^{r+1}) \to \underbrace{H_0(K_\bullet^r)}_{A/(t_1,\ldots,t_r)} \xrightarrow{\delta} \underbrace{H_0(K_\bullet^r)}_{A/(t_1,\ldots,t_r)} \to H_0(K_\bullet^{r+1}) \to 0$$

Dunque ci resta da capire come sono fatti i due pezzi senza le parentesi graffe sotto. Ripercorrendo la definizione della mappa di bordo nella successione esatta lunga in omologia viene fuori che $\delta(x) = t_{r+1}x$, il che mostra simultaneamente che δ è iniettiva, e quindi $H_1(K_\bullet^{r+1}) = 0$, e che $H_0(K_\bullet^{r+1}) \cong A/(t_1, \ldots, t_{r+1})$. □

Osservazione C.12. Lo stesso Teorema vale anche nel caso locale se $\mathfrak{m} = (t_1, \ldots, t_r)$ e le mappe

$$\cdot t_i\colon A/(t_1, \ldots, t_{i-1}) \to A/(t_1, \ldots, t_{i-1})$$

sono iniettive. Nel caso in cui A è locale regolare è effettivamente possibile trovare un tale insieme di generatori, quindi per gli A locali regolari $\text{gl-dim}(A) = \dim A$.

Esercizio C.13. Sia $A = \mathbb{K}[t_1, \ldots, t_n]$ e M finitamente generato. Allora M ha una risoluzione proiettiva/libera finita.

[16] Facendo un po' di conti.

[17] Vedi Teorema 7.39, dove però il diagramma è ruotato e riflesso: qui le mappe orizzontali sono quelle *dei* complessi e quelle verticali quelle *fra* i complessi, lì al contrario.

Bibliografia

[1] P. Aluffi, *Algebra: Chapter 0*
AMS Graduate Studies in Mathematics, Volume 104, 2009

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*
Addison-Wesley Series in Mathematics, 1969

[3] P. L. Clarke, *Commutative Algebra*,
`http://math.uga.edu/~pete/integral.pdf`

[4] G. d'Antonio, *Appunti del Corso di Elementi di Algebra Superiore*,
`http://www.dm.unipi.it/~gaiffi/IstAlgebra/algsup2-2.pdf`

[5] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer (1995)

[6] P. J. Hilton, U. Stammbach, *A Course in Homological Algebra*, Second Edition, Springer Graduate Text in Mathematics, (1997)

[7] T. Jech, *Set Theory*, The Third Millenium Edition,
Springer Monographs in Mathematics (2003)

[8] S. Maggiolo, *Appunti del corso: Elementi di algebra superiore 2*,
`http://poisson.phc.unipi.it/~maggiolo/wp-content/uploads/2008/12/elementi_di_algebra_superiore_2.pdf`

[9] Mathematics Stack Exchange, *Natural Transformation between covariant and contravariant functor*, consultato il 03/04/15,
`http://math.stackexchange.com/questions/120342/natural-transformation-between-covariant-and-contravariant-functor`

[10] MathOverflow, *Errata for Atiyah-Macdonald*, consultato il 17/03/15,
`http://mathoverflow.net/questions/42241/errata-for-atiyah-macdonald`

[11] MathOverflow, *Why not _co_free modules?*, consultato il 07/04/15,
`http://mathoverflow.net/questions/38085/why-not-co-free-modules`

[12] H. Matsumura, *Commutative Ring Theory*,
Cambridge Studies in Advanced Mathematics (1989)

[13] H. Matsumura, *Commutative Algebra*,
Mathematics lecture note series, 56 (1980)

[14] R. Mennuni, *Appunti del Corso di Elementi di Geometria Algebrica*,
`http://poisson.phc.unipi.it/~mennuni/appuntiEGA.pdf`

[15] nLab, *Single-sorted definition of a category*, `http://ncatlab.org/nlab/show/single-sorted+definition+of+a+category`

[16] S. Schröer, *Baer's Result: The Infinite Product of the Integers Has No Basis*, `http://www.math.uni-duesseldorf.de/~schroeer/publications_pdf/infinite_product-1.pdf`

[17] A. Seidenberg, *On the dimension theory of rings. II*, Pacific Journal of Mathematics 4: 603–614 (1954)

[18] S. Shelah, *Infinite Abelian groups, Whitehead problem and some constructions*, Israel Journal of Mathematics 18 (3): 243–256 (1974)

[19] S. Shelah, *Whitehead groups may not be free, even assuming CH. I*,
Israel Journal of Mathematics 28 (3): 193–203 (1977)

[20] S. Shelah, *Whitehead groups may not be free, even assuming CH. II*,
Israel Journal of Mathematics 35 (4): 257–285 (1980)