Disclaimer

Questi appunti nascono ad uso e consumo degli autori, che li stanno TEXando in diretta e successivamente risistemando durante il corso di Istituzioni di Algebra tenuto dal professor Gaiffi[1] presso l'Università di Pisa durante il primo semestre dell'anno accademico 2014/2015. Come conseguenza possono essere *molto* poco chiari, difettare di qualcosa, eccetera eccetera, e in particolare *non* sono gli appunti ufficiali del corso. Sentitevi liberi di insultarci, segnalare sviste, errori, imprecisioni, carenze eccetera presso `mennuni@mail.dm.unipi.it` o `sircana@mail.dm.unipi.it`. Ogni contributo è bene accetto.

L'ultima versione di questi appunti e il relativo sorgente sono disponibili presso `poisson.phc.unipi.it/~mennuni/`. Questa versione è stata compilata il 20 marzo 2015. La maniera migliore che ci viene in mente per sapere cosa cambia rispetto alla versione precedente che avete scaricato è scaricarsi anche i sorgenti e tiraci sopra un `diff`. Se non avete il sorgente della versione precedente potete provare a usare `diffpdf`, ma sinceramente noi non ci abbiamo mai provato.

Rosario "Mufasa" Mennuni — Carlo Sircana

[1] Con qualche lezione tenuta dal professor Maffei.

Indice

Capitolo 1

Estensioni Intere

Il comportamento delle estensioni e delle contrazioni di ideali tramite omomorfismi di anelli è piuttosto caotico ed è difficile poter avere risultati a priori. Dei risultati si possono però ottenere considerando 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* $p \in A[x]$.

Il parallelo è con la nozione di algebricità vista per estensioni di campi; lavorando con anelli è importante che il polinomio sia monico. Per esempio, se consideriamo $\mathbb{Z} \subseteq \mathbb{Q}$ gli x interi su $\mathbb{Z}$ sono tutti e soli gli elementi di $\mathbb{Z}$. In realtà possiamo enunciare un risultato equivalente per ogni UFD:

Proposizione 1.2. Sia A un UFD e sia K il suo campo dei quozienti. Allora gli elementi di K interi su A sono tutti e soli gli elementi di A.

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,

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

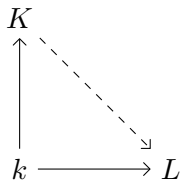
da cui

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

Di conseguenza, $q \mid p^n$; poiché siamo in un UFD e $(q, p) = 1$, si ha $q \mid p$ da cui $q = 1$.

□

L'obiettivo è ottenere una generalizzazione della proprietà di sollevamento come quella riportata nel diagramma:



dove L è algebricamente chiuso e K è un estensione algebrica. Vorremmo mostrare che si ha la stessa proprietà quando K è un'estensione intera di k.

Mostriamo ora delle definizioni equivalenti di elemento intero:

Teorema 1.3. Sono equivalenti:

1. $x \in B$ 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*[1] M che è finitamente generato come A-modulo.

Dimostrazione.

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

$(2 \Rightarrow 3)$ Basta prendere $C = A[x]$.

$(3 \Rightarrow 4)$ Basta prendere $M = C$. Questo è fedele perché contiene 1, e se non fosse fedele dovrebbe essere $p(x) \cdot 1 = 0$, e quindi $p = 0$.

$(4 \Rightarrow 1)$ Ricordiamo che se M è un A-modulo finitamente generato, e $\varphi = x\cdot$ è un omomorfismo di A-moduli, per Cayley-Hamilton $\varphi^n + \sum a_i \varphi^i = 0$, con $a_i \in A$. Se l'operatore $(x^n + \sum a_i x^i = 0)\cdot$ è nullo, dato che M è fedele deve essere $x^n + \sum a_i x^i = 0$.

□

I seguenti Corollari sono analoghi ai risultati che si hanno per le estensioni algebriche.

Corollario 1.4. Siano $x_1, \ldots, x_n \in B$ interi su A. Allora $A[x_1, \ldots, x_n]$ è un A-modulo finitamente generato.

[1] Cioè $\mathrm{Ann}(M) = 0$.

Corollario 1.5. 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 1.3. Allo stesso modo, si mostra che $xy \in C$. □

Definizione 1.6. 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.

Proposizione 1.7. 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 $x^n + \sum b_i x^i = 0$. Considerando l'anello $B' = A[b_0, \ldots, b_{n-1}]$ abbiamo che x è intero su B', e allora $B'[x]$, che è sicuramente finitamente generato come B'-modulo, è $A[b_0, \ldots, b_{n-1}][x]$, ed è quindi anche un A-modulo finitamente generato. Inoltre $A[x] \subseteq B'[x]$ e basta utilizzare il Teorema. □

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, cioè l'idempotenza della chiusura integrale. La chiusura integrale si comporta bene anche rispetto a operazioni fra anelli:

Proposizione 1.8. Sia $A \subseteq B$, B intero su A, $\mathfrak{q}$ 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 $\mathfrak{q}$,

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

dove abbiamo sfruttato che $\mathfrak{p} = A \cap \mathfrak{q}$. □

Proposizione 1.9. 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 $\frac{x}{s}$ 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 $(st)^n$. Notiamo subito che (bt) è intero su A e quindi appartiene a C. Ma allora $b/s = (bt)/(st) \in S^{-1}C$. □

1.1 I Teoremi di Cohen-Seidenberg

Studiamo ora gli ideali primi delle estensioni intere: ci chiediamo se riusciamo a trovare un ideale tale che $\mathfrak{q}^c = \mathfrak{p}$.

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

Questo è essenziale per le proprietà di estensione che vorremmo dimostrare, perché $\mathfrak{q}$ con tale proprietà sarà il candidato nucleo dell'omomorfismo.

Proposizione 1.10. Siano $A \subseteq B$ domini e B intero su A. Allora B è un campo se e solo se A lo è.

Dimostrazione. Se B è un campo prendiamo $0 \neq x \in A$. Sicuramente $x^{-1} \in B$, e siccome l'estensione è intera possiamo scrivere $(x^{-1})^m + \sum a_i (x^{-1})^i = 0$, 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. A è un dominio, dunque $a_0 \neq 0$ perché altrimenti potremmo raccogliere y nell'equazione e ridurre il grado della relazione. Portando a secondo membro a_0 e dividendo per esso, ricordando che a_0 è invertibile perché elemento non nullo di A, otteniamo

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

e dunque abbiamo trovato un inverso di y.

□

Corollario 1.11. 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. $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$; basta allora applicare la Proposizione precedente, dato che il quoziente per un ideale massimale è un campo. □

Corollario 1.12. 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 abbiamo

$$S^{-1}\mathfrak{p} \subseteq S^{-1}A \subseteq S^{-1}B$$

Notiamo che $S^{-1}\mathfrak{q}_0$ e $S^{-1}\mathfrak{q}_1$ si contraggono entrambi a $S^{-1}\mathfrak{p}$ e sono dunque massimali per il corollario precedente. Abbiamo allora $S^{-1}\mathfrak{q}_0 = S^{-1}\mathfrak{q}_1$, poiché $S^{-1}\mathfrak{q}_0 \subseteq S^{-1}\mathfrak{q}_1$ e sono entrambi massimali. 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. Dunque $\mathfrak{q}_0 = \mathfrak{q}_1$. □

Teorema 1.13 (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. Consideriamo il diagramma

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

e prendiamo $\mathfrak{m} \in \mathrm{SpecMax}(S^{-1}B)$. Per quanto visto la sua contrazione in $S^{-1}A = A_\mathfrak{p}$ è massimale, e quindi è $S^{-1}\mathfrak{p}$ e questo viene contratto a $\mathfrak{p}$. D'altra parte $\mathfrak{m}$ si contrae in B a un $\mathfrak{q} \in \mathrm{Spec}(B)$, e per la commutatività del diagramma $\mathfrak{q}^c = \mathfrak{p}$. □

Questo appena dimostrato non è altro che il passo base della dimostrazione del seguente teorema:

Teorema 1.14 (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

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

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

Dimostrazione. Per induzione, possiamo ridurci al caso $n = 2$ e $m = 1$. Siano $\bar{A} = A/\mathfrak{p}_1$ e $\bar{B} = B/\mathfrak{q}_1$. Abbiamo che $\bar{B}$ è intero su $\bar{A}$, e per il teorema precedente troviamo $\bar{\mathfrak{q}}^c = \bar{\mathfrak{p}_2}$. Detta $\pi\colon B \to B/\mathfrak{q}_1$, basta porre $\mathfrak{q}_2 = \pi^{-1}(\bar{\mathfrak{q}})$ per ottenere la tesi. □

Possiamo ora dimostrare il risultato di estensione degli omomorfismi preannunciato:

Teorema 1.15. Sia $\varphi\colon A \to L$, con L algebricamente chiuso, sia B intero su A. Allora φ si estende ad un omomorfismo $\tilde{\varphi}\colon B \to L$.

Dimostrazione. Supponiamo dapprima che $\operatorname{Ker}\varphi = \mathfrak{m} \in \operatorname{SpecMax}(A)$. Per il Teorema del Lying Over esiste $\mathfrak{M} \in \operatorname{SpecMax}(B)$ tale che $\mathfrak{M}^c = \mathfrak{m}$. Fattorizziamo φ come $A \to {}^{A}\!/_{\mathfrak{m}} \xrightarrow{\bar{\varphi}} L$ e otteniamo

$$\begin{array}{ccccc} B & \xrightarrow{\pi} & {}^{B}\!/_{\mathfrak{M}} & & \\ \uparrow & & \uparrow & \searrow^{\tilde{\tilde{\varphi}}} & \\ A & \xrightarrow[\pi]{} & {}^{A}\!/_{\mathfrak{m}} & \xrightarrow[\bar{\varphi}]{} & L \end{array}$$

dato che un'estensione intera di campi è algebrica esiste $\tilde{\tilde{\varphi}}\colon B/\mathfrak{M} \to L$ che estende $\bar{\varphi}$. Per concludere questo caso, basta allora considerare $\tilde{\varphi} = \tilde{\tilde{\varphi}} \circ \pi$.

Se invece $\mathfrak{p} = \operatorname{Ker}\varphi$ è un ideale primo non massimale[2], localizziamo con $S = A \setminus \mathfrak{p}$ e troviamo $\hat{\varphi}\colon S^{-1}A \to L$. Ora $\operatorname{Ker}\hat{\varphi}$ è massimale e per quanto visto sopra possiamo estendere a $\tilde{\hat{\varphi}}$, e componendo abbiamo l'estensione sperata. □

Questo fornisce una dimostrazione alternativa di una forma debole del Nullstellensatz:

Teorema 1.16. Sia $\mathbb{K}$ un campo, $B = \mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra finitamente generata. Se B è un campo allora è un'estensione algebrica finita di $\mathbb{K}$.

Siano ora A un dominio, K il suo campo dei quozienti e L un'estensione di K. Ha senso chiedersi se la nozione di elemento algebrico su K sia legata a quella di elemento intero su A. Infatti, se $x \in L$ è algebrico su K sappiamo che esiste $f \in K[t]$ il suo polinomio minimo. Se $f(t) = t^n + \sum a_i t^i$ e tutti gli a_i sono in a allora x è intero su A. Purtroppo il viceversa in generale è falso. 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 è a coefficienti in A, ma x è comunque intero su A. Infatti

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

[2]Ricordiamo che la contrazione di primi è prima.

La proprietà è vera se si aggiunge la seguente ipotesi:

Definizione 1.17. Un dominio A si dice *integralmente chiuso* o *normale* se per ogni $x \in K$ se x è intero su A allora $x \in A$.

Proposizione 1.18. Sia A un dominio integralmente chiuso e sia K il suo campo dei quozienti. Allora $\alpha \in \bar{K}$ è intero su A se e solo se il polinomio minimo di α su K appartiene a $A[x]$.

Dimostrazione. Se il polinomio minimo di α su K è a coefficienti in A allora α è intero su A.
Viceversa, sia a intero su A e sia

$$p(t) = t^n + \sum a_i t^i$$

una relazione di interezza di grado minimo. Sia μ_a il polinomio minimo di a su K. Se mostriamo che ogni radice del polinomio minimo μ_a è intera su A, allora il polinomio minimo è a coefficienti in A. Infatti i coefficienti sarebbero combinazioni delle radici e dunque sarebbero elementi interi su A appartenenti a K; ma A è integralmente chiuso in K e dunque sarebbe a coefficienti in A. Questo è chiaro visto che per definizione di polinomio minimo $\mu_a \mid p$ e dunque ogni radice di μ_a è anche radice di p. Di conseguenza p è una relazione di interezza per ogni radice di μ_a da cui la tesi. □

Con queste ipotesi vale anche un teorema analogo al Going Up per le catene discendenti finite di ideali primi. In generale, infatti, una simile proprietà non vale. Consideriamo la cubica in $\mathbb{C}^3$ data da $f(x, y, z) = y^2 - x^3 - x^2$. L'omomorfismo

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

con $x \mapsto t^2 - 1$ e $y \mapsto t^3 - t^2$ 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 $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.
Studiamo allora la natura di questi anelli:

Lemma 1.19. 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 $S = A \setminus \mathfrak{p}$ per la Proposizione 1.9 si ha

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

e dunque A_p è integralmente chiuso.

($2 \Rightarrow 3$) Ovvio.

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

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

Basta mostrare che $M \subset A$ per concludere. Sia dunque per assurdo $x \in M \setminus A$ e consideriamo l'ideale

$$I = \{a \in A \mid ax \in A\}$$

che è proprio perché $x \notin A$. Esiste allora un ideale massimale $\mathfrak{m}$ tale che $I \subset \mathfrak{m}$. 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 $s \notin I$. Ciò è assurdo perché $sx = y \in A$.

□

L'interezza può essere trattata anche rispetto ad ideali:

Definizione 1.20. 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 1.21. Sia $I \subset A \subset B$ 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. Mostriamo l'inclusione $\overline{I} \subseteq \sqrt[\overline{A}]{\overline{A}I}$. Se $x \in \overline{I}$, allora x è intero su A e dunque esiste una relazione $x^n = \sum a_i x^i \in \overline{A}I$. Quindi $x \in \sqrt[\overline{A}]{\overline{A}I}$. Viceversa, supponiamo che $x \in \sqrt[\overline{A}]{\overline{A}I}$. Allora $x^n = \sum a_i x_i \in \overline{A}I$ con gli $a_i \in I$ e gli $x_i \in \overline{A}$. Consideriamo l'A-modulo $M = A[x_1, \dots, x_n]$. M è finitamente generato come A-modulo; definiamo l'omomorfismo di A-moduli $\varphi(u) = x^n u$. Notiamo che $\varphi(M) \subset IM$: per il teorema di Hamilton-Cayley esistono $b_1, \dots, b_z \in I$ tali che $\varphi^z + \sum b_i \varphi^i = 0$. Dunque $x^{nz} + \sum b_i x^{ni} = 0$ da cui la tesi. □

È vero un analogo della Proposizione 1.18:

Proposizione 1.22. 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. La dimostrazione è identica una volta osservato che gli elementi di K interi su I sono $\sqrt{I}$. □

Per dimostrare il teorema del Going-Down, abbiamo bisogno del seguente lemma:

Lemma 1.23. 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 $\mathfrak{q}$ di B se e solo se $\mathfrak{p}^{ec} = \mathfrak{p}$.

Dimostrazione.

$\Rightarrow$ Dalla relazione $\mathfrak{q}^c = \mathfrak{p}$, ricaviamo $\mathfrak{p}^{ec} = (q^c)^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = p$, come voluto.

$\Leftarrow$ Sia $S = A \setminus \mathfrak{p}$. Consideriamo il diagramma

$$\begin{array}{ccc} A & \longrightarrow & S^{-1}A \\ \downarrow & & \downarrow \\ B & \longrightarrow & S^{-1}B \end{array}$$

Dato che $\mathfrak{p}^{ec} = \mathfrak{p}$, $\mathfrak{p}^e$ non interseca S e dunque in $S^{-1}B$ $\mathfrak{p}^e$ è un ideale proprio. Dunque è contenuto in un massimale $\mathfrak{q}$ di $S^{-1}B$. Per commutatività del diagramma, la contrazione di $\mathfrak{q}$ in $S^{-1}A$ deve essere un ideale primo di $S^{-1}A$ che contiene $\mathfrak{p}$ e dunque coincide con $\mathfrak{p}$. Dunque $\mathfrak{q}^c = \mathfrak{p}$.

□

Teorema 1.24 (Going Down)**.** Siano $A \subset B$ domini con A integralmente chiuso e B intero su A. Siano $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} A$ tali che $\mathfrak{p}_1 \subset \mathfrak{p}_2$ e sia $\mathfrak{q}_2 \in \operatorname{Spec} B$ tale che $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Allora esiste $\mathfrak{q}_1 \in \operatorname{Spec} B$ tale che $\mathfrak{q}_1 \subset \mathfrak{q}_2$ e $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

Dimostrazione. Sia $S = B \setminus \mathfrak{q}_2$. Per il Lemma 1.23, basta mostrare che $(S^{-1}B)\mathfrak{p}_1 \cap A = \mathfrak{p}_1$.

$$A \longrightarrow B \longrightarrow S^{-1}B$$

Mostriamo che $J = (S^{-1}B)\mathfrak{p}_1$ soddisfa la relazione $J \cap A = \mathfrak{p}_1$. Sia $x \in J \cap A$. Allora $x \in S^{-1}(B\mathfrak{p}_1) \cap A$, per cui $x = y/s$ con $y \in B\mathfrak{p}_1$ e $s \in B \setminus \mathfrak{q}_2 = S$. Poiché y è intero su A, il suo polinomio minimo su K $f(t) = t^n + \sum a_i t^i$ è a coefficienti $a_i \in A$, e dato che $y \in B\mathfrak{p}_1 \subset \sqrt{B\mathfrak{p}_1}$ sappiamo anche che y è intero su $\mathfrak{p}_1$. Calcoliamo il polinomio minimo di $s = y/x$ su K. Dalla relazione

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

dividendo per x^n troviamo

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

Il polinomio $p(t) = t^n + \sum a_i t^i / x^{n-i} \in K[t]$ è il polinomio minimo di s su K; se ce ne fosse uno di grado minore ne otterremmo uno di grado minore anche per y moltiplicando per una potenza di x opportuna[3]. Ricordando che $s \in B \setminus \mathfrak{q}_2 \subset B$, si ottiene che s è intero su A, per cui $b_i = a_i/x^{n-i} \in A$ e $\mathfrak{p}_i \ni a_i = x^{n-1}\mathfrak{b}_i$. Se fosse $x \notin \mathfrak{p}_1$ allora $b_i \in \mathfrak{p}_1$, quindi s sarebbe intero anche su $\mathfrak{p}_1$, per cui avremmo l'assurdo

$$s \in \sqrt{B\mathfrak{p}_1} \subset \sqrt{B\mathfrak{p}_2} \subset \sqrt{\mathfrak{q}_2} = \mathfrak{q}_2$$

□

Interi Quadratici Sia $d \in \mathbb{Z}$ libero da quadrati. Calcoliamo la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$. 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 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. Per il Lemma 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.

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 $f(x) = (x - \alpha)(x - \sigma(\alpha)) = x^2 - (\alpha + \sigma(\alpha)) - \alpha\sigma(\alpha)$, per cui se α è intero su $\mathbb{Z}$ abbiamo $\alpha + \sigma(\alpha), \alpha\sigma(\alpha) \in \mathbb{Z}$. Definiamo $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ rispettivamente *traccia* e *norma* di α, denotate con $T(\alpha)$ e $N(\alpha)$. Abbiamo dunque mostrato che in queste estensioni, se α è intero su $\mathbb{Z}$, $T(\alpha) \in \mathbb{Z}$ e $N(\alpha) \in \mathbb{Z}$; vale anche il viceversa, cioè se $T(\alpha) \in \mathbb{Z}$ e $N(\alpha) \in \mathbb{Z}$, allora α è intero su $\mathbb{Z}$.

Lemma 1.25. Sia α intero su $\mathbb{Z}$, $\alpha = x + y\sqrt{d}$. Allora vale una e una sola delle seguenti:

[3] Ad esempio da $s^2 = 1$ otterremmo $y^2 = x^2$.

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

Dimostrazione. Notiamo che

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

Supponiamo ora $x \in \mathbb{Z}$. Allora $x^2 \in \mathbb{Z}$ e quindi $dy^2 \in \mathbb{Z}$. Supponiamo $y = s/t$, con $(s,t) = 1$. Se $ds^2/t^2 \in \mathbb{Z}$, $t^2 \mid ds^2$, e questo, visto che d è squarefree, implica $t = 1$ e $y \in \mathbb{Z}$. 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 $4 \mid s^2 - 4dy^2$. Dunque $y^2 \notin \mathbb{Z}$ e dunque 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 1.26. 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 $1 - d \equiv 0 \pmod 4$.

Teorema 1.27. 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 (uno è per $d = -3$).

1.2 Lemma di Normalizzazione di Noether

Passiamo ora a considerare estensioni di anelli generiche. Il seguente teorema permette di scomporle individuando una parte trascendente e una intera:

Lemma 1.28 (di Normalizzazione di Noether)**.** Sia $\mathbb{K}[x_1, \ldots, x_n]$ una $\mathbb{K}$-algebra finitamente generata[4]. 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 (J). Vogliamo ridurre il numero di variabili per sostituzione: siano $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0\}$ e prendiamo

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

per poi sostituire nell'equazione (1.1) x_i con $y_i' + x_1^{m_1}$. Consideriamo il vettore $(m) = (1, m_2, \ldots, m_n)$ con le operazioni $(m)(J) = j_1 + m_2 j_2 + \ldots + m_n j_n$. Otteniamo

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

Vogliamo dire che x_1 è intero su $\mathbb{K}[y_2', \ldots, y_n']$. Poiché ogni x_i è intero su $\mathbb{K}[x_1, y_2', \ldots, y_n']$ (per $i > 1$), si ha che $\mathbb{K}[x_1, \ldots, x_n]$ è intero sull'anello $\mathbb{K}[x_1, y_2', \ldots, y_n']$. Supponiamo di aver scelto (m) in modo che nella somma non vi siano cancellazioni; allora $\mathbb{K}[x_1, y_2', \ldots, y_n']$[5] è intero su $\mathbb{K}[y_2', \ldots, y_n']$. Possiamo allora procedere per induzione sul numero di generatori.

Rimane da mostrare che è possibile scegliere (m) in maniera da non avere cancellazioni di x_1 nell'equazione sopra. In altre parole dobbiamo rendere iniettiva la mappa $(J) \mapsto (m)(J)$. Per questo, sia $k = 1 + \max_J J_i$. Preso allora $m = (1, k, k^2, \ldots, k^{n-1})$, si ha la tesi, per unicità di scrittura dei naturali in base k. □

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

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

[5] $c_j \in \mathbb{K}$ e quindi possiamo rendere il polinomio monico senza problemi.

Il lemma di Normalizzazione di Noether permette di sviluppare la teoria in varie direzioni. È utile per esempio per dare la nozione di base di trascendenza:

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 lemma di Normalizzazione di Noether 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". Questo vale effettivamente sotto alcune ipotesi sulla $\mathbb{K}$-algebra.

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. Sia $W_1 \notin \{Y_1, \ldots, Y_r\}$ (se non c'è la tesi è vera) 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 uno degli Y_i (senza perdita di generalità 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. Di conseguenza, $\mathbb{K}(x_1, \ldots, x_n)$ è algebrico su $\mathbb{K}(Y_1, \ldots, Y_r, W_1)$ perché gli Y_i sono una base di trascendenza e quest'ultimo è algebrico su $\mathbb{K}(Y_2, \ldots, Y_r, W_1)$. Consideriamo ora W_2; questo è un elemento di $\mathbb{K}(x_1, \ldots, x_n)$ ed è quindi algebrico su $\mathbb{K}(Y_2, \ldots, Y_r, W_1)$. 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 $\mathbb{K}(x_1, \ldots, x_n)$ è algebrico su $\mathbb{K}(W_1, \ldots, W_r)$. Dunque $W_1, \ldots, W_r, W_{r+1}$ sono algebricamente dipendenti, 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.

Esempio 1.35. In $\mathbb{K}[X] \times \mathbb{K}[Y, Z]$, sia $\{A = (X, 0)\}$ che $\{(0, Y) \times (0, Z)\}$ sono insiemi algebricamente indipendenti massimali, ma hanno cardinalità diversa. Sia infatti $D = (p(X), q(Y, Z))$ un elemento del prodotto tale che l'insieme $\{A, D\}$ sia algebricamente indipendente. Se $p(X) = \sum a_i X^i$, allora

$$\left((p(X), q(Y, Z)) - \sum a_i (X, 0)^i\right)(X, 0) = (0, q(X, Z))(X, 0) = 0$$

e dunque $\{A, D\}$ è algebricamente dipendente, contro quanto supposto.

1.3 Lemma di Selberg e Residuale Finitezza

I teoremi di estensione di omomorfismi possono essere raffinati:

Teorema 1.36. Sia $A \subseteq B$ dominio che è anche una A-algebra finitamente generata, e sia $b \in B \setminus \{0\}$. Allora esiste $a \in A \setminus \{0\}$ tale che ogni omomorfismo $\alpha \colon A \to L$, con L algebricamente chiuso, per il quale $\alpha(a) \neq 0$ può essere esteso ad un omomorfismo $\beta \colon B \to L$ tale che $\beta(b) \neq 0$.

Dimostrazione. Procediamo per induzione; ppossiamo 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 $k(A)$. In questa situazione, $b \in B$ si può scrivere come $b = \sum_{i=0}^{n} a_{n-i} x^i$, con gli $a_i \in A$ e $a_0 \neq 0$. Scegliamo $a = a_0$ e sia $\alpha \colon A \to L$ un omomorfismo tale che $\alpha(a) \neq 0$. Consideriamo il polinomio in $L[t]$

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

p ha esattamente n radici in L perché questo è algebricamente chiuso. In particolare L è infinito, e quindi esiste $y \in L$ che non è radice. Basta allora estendere l'omomorfismo con $x \mapsto y$ per avere la tesi.

Occupiamoci ora del primo caso. Abbiamo

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

Dato che $b \in k(A)[x]$ sappiamo che b è algebrico su $k(A)$; possiamo allora trovare una relazione $\sum_{i=0}^{n} d_i b^i = 0$, dove $d_i \in A$ con $d_n \neq 0$. Notiamo che poiché siamo in un dominio possiamo anche supporre $d_0 \neq 0$. Moltiplicando per $b^{-n} \in k(B)$ otteniamo

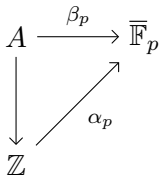
$$d_0 b^{-n} + \ldots + d_n = 0$$

Ricordiamo che x è algebrico su $k(A)$, e quindi soddisfa una relazione del tipo $\sum_{j=0}^{m} c_{m-i} x^i$, con i $c_i \in A$ e $c_0 \neq 0$. Scegliamo $a = d_0 \cdot c_0 \in A$ e sia $\alpha\colon A \to L$ tale che $\alpha(a) \neq 0$. Sappiamo che α può essere esteso a $\alpha'\colon S^{-1}A \to L$, dove $S = \{a^i \mid i \in \mathbb{N}\}$. In questo modo abbiamo reso invertibili sia d_0 che c_0. Abbiamo $S^{-1}A = A[a^{-1}]$, e notiamo che $A[a^{-1}][b^{-1}]$ è intera su $A[a^{-1}]$ poiché è possibile ora invertire il termine di testa nella relazione di sopra. Si può estendere dunque α' ad $\alpha''\colon A[a^{-1}][b^{-1}] \to L$. Possiamo estendere ulteriormente alla chiusura integrale C di $A[a^{-1}]$ in $k(B)$ per interezza, ottenendo un omomorfismo $\alpha'''\colon C \to L$.
Ci basta ora mostrare che $B \subseteq C$ e che $b^{-1} \in C$: la restrizione di α''' sarà l'omomorfismo cercato. Infatti, se $b, b^{-1} \in C$, allora $\beta(bb^{-1}) = \beta(1) = 1$ e dunque $\beta(b) \neq 0$. Dato che $B = A[x]$ e che x è intero su $A[a^{-1}]$ otteniamo $B \subseteq C$ per definizione di chiusura integrale. D'altra parte $b^{-1} \in C$ perché è intero su $A[a^{-1}]$. Vale dunque la tesi con $\beta = \alpha'''_{\restriction B}$.
Supponiamo ora $B = A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ e sia $b \in B$. Allora, ripetendo il passo base, esiste $s \in A[x_1, \ldots, x_{n-1}]$ tale che ogni omomorfismo $\varphi\colon A[x_1, \ldots, x_{n-1}] \to L$ si estende a un omomorfismo $\tilde{\varphi}\colon B \to L$ tale che $\tilde{\varphi}(b) \neq 0$. Per ipotesi induttiva, esiste $t \in A$ tale che ogni omomorfismo $\psi\colon A \to L$ tale che $\psi(t) \neq 0$ si estende a un omomorfismo $\tilde{\psi}\colon A[x_1, \ldots, x_{n-1}] \to L$ tale che $\tilde{\psi}(s) \neq 0$. Di conseguenza, scelto $a = t$, si ha la proprietà di estensione desiderata.

□

Teorema 1.37. Sia A un sottoanello di $\mathbb{C}$ che sia una $\mathbb{Z}$-algebra finitamente generata $\mathbb{Z}[a_1, \ldots a_m] \subseteq \mathbb{C}$. Allora ogni sottogruppo di $\mathrm{GL}(n, A)$ ha un sottogruppo normale di indice finito libero da torsione.

Dimostrazione. Per ogni $p \in \mathbb{Z}$ primo, prendiamo $\alpha_p\colon \mathbb{Z} \to \overline{\mathbb{F}}_p$ ottenuta componendo la proiezione al quoziente con l'immersione nella chiusura algebrica. Poniamo $b = 1$. Esiste $m \in \mathbb{Z}$ tale che se $\alpha\colon \mathbb{Z} \to \overline{\mathbb{F}}_p$ è tale che $\alpha(m) \neq 0$ possiamo estendere α ad A; siamo infatti nelle ipotesi del teorema precedente, visto che ogni sottoanello di un dominio è un dominio. Poiché $m \in \mathbb{Z}$, ha finiti primi che compaiono nella fattorizzazione; abbiamo dunque infinite mappe α_p tali che $\alpha_p(m) \neq 0$ e possiamo estendere ognuno di queste ad A.



$\operatorname{Ker}\beta_b$ è un ideale proprio di A, e $\operatorname{Ker}\beta_p \cap \mathbb{Z} = p\mathbb{Z}$, dove l'uguaglianza vale per massimalità. Inoltre β_p induce una mappa iniettiva $A/\operatorname{Ker}\beta_p \to \overline{\mathbb{F}}_p$. $A/\operatorname{Ker}_{\beta_p}$ è una $\mathbb{F}_p$-algebra finitamente generata. Detti $\bar{a_1}, \dots \bar{a_n}$ i generatori, si ha, per definizione di $\bar{\mathbb{F}}_p$, che $\beta_p(\bar{a_i}) \in \mathbb{F}_{p^{s_i}}$. Sia $k = mcm(s_i \mid i = 1 \dots n)$; sicuramente l'immagine di A è contenuta in $\mathbb{F}_{p^k}$. Dunque $A/\operatorname{Ker}\beta_p$ è finito, ed è un dominio perché vive in un campo. Ogni dominio finito è però un campo; quindi $\operatorname{Ker}\beta_p$ è massimale e lo chiamiamo $\mathfrak{m}_p$.

Consideriamo ora l'omomorfismo di gruppi

$$\pi_p \colon \mathrm{GL}(n, A) \longrightarrow \mathrm{GL}\left(n, {}^{A}\!/_{\mathfrak{m}_p}\right)$$

che data una matrice $A = (a_{i,j})$ restituisce la matrice $\bar{A} = (\bar{a}_{ij})$. Il suo nucleo $\operatorname{Ker}\pi_p$ è un sottogruppo normale di $\mathrm{GL}(n, A)$ e ha indice finito, perché $\mathrm{GL}(n, A)/\operatorname{Ker}\pi_p$ si immerge in un gruppo finito. Dato ora Γ sottogruppo di $\mathrm{GL}(n, A)$ 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 m e ripetiamo la costruzione. Otteniamo così un sottogruppo $\Gamma_q = \Gamma \cap \operatorname{Ker}\pi_q$. Il sottogruppo $\Gamma_p \cap \Gamma_q$ è normale e di indice finito; mostriamo che è libero da torsione.

Supponiamo di avere una matrice $g \in \Gamma_p \cap \Gamma_q$ che abbia ordine r, che possiamo supporre primo. Dato che $g^r = \mathrm{id}$, il suo polinomio minimo divide $t^r - 1$, che ha in $\mathbb{C}$ tutte radici distinte. Di conseguenza, g è diagonalizzabile e siano $\lambda_1, \dots, \lambda_n$ i suoi autovalori, radici r-esime dell'unità. Notiamo che almeno uno di questi deve esserne una radice r-esima primitiva ζ_r, altrimenti l'ordine di g sarebbe minore di r.

Consideriamo allora $B = A[\zeta_r]$, che è intero su A (è addirittura intero su $\mathbb{Z}$). Abbiamo $\mathfrak{m}_p \subseteq A$ e per il Lying Over esiste un ideale massimale $\mathfrak{q}_p$ tale che $\mathfrak{q}_p \cap A = \mathfrak{m}_p$. 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 $g \in \operatorname{Ker}(\pi_p)$. Dunque

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

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

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

$$1 = \zeta_r^r = (1+x)^r = 1 + rx + \binom{r}{2}x^2 + \ldots = 1 + x(r+y)$$

dove $y \in \mathfrak{q}_p$. Dunque $x(r+y) = 0$ ma per costruzione $x \neq 0$; infatti $1+x = \zeta_r$. Poiché siamo in un dominio, $r = -y$ e $r \in \mathfrak{q}_p \cap \mathbb{Z} = p\mathbb{Z}$. La stessa costruzione può però essere fatta con $\mathfrak{q}$. Siccome r è primo si ha l'assurdo $r = p \neq q = r$. □

Dimostriamo ora il teorema di Selberg:

Teorema 1.38 (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.

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

Teorema 1.39. 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 $\varphi_g(g) \neq 1$.

Dimostrazione. Sia $\gamma \in G < \mathrm{GL}(n, \mathbb{C})$. Come fatto in precedenza, siano $a_1, \ldots a_m$ i coefficienti delle matrici $g_1, \ldots g_n, g_1^{-1}, \ldots, g_n^{-1}$ che generano G e sia $A = \mathbb{Z}[a_1, \ldots, a_m]$.

Consideriamo le proiezioni $\pi_p \colon \mathrm{GL}(n, A) \to \mathrm{GL}(n, A/\mathfrak{m}_p)$. Supponiamo dapprima che la matrice non sia diagonale; esiste allora $b \neq 0$ elemento della matrice fuori dalla diagonale. Prendiamo questo b come b del Teorema 1.36, ottenendo $m \in \mathbb{Z}$ tale che per ogni $\alpha \colon \mathbb{Z} \to L$, con L campo algebricamente chiuso, valga $\alpha(m) \neq 0$. Prendiamo ora p tale che $p \nmid m$. Abbiamo come prima $\mathrm{GL}(n, A) \xrightarrow{\varphi} \mathrm{GL}(n, A/\mathfrak{m}_p)$ gruppo finito, che si restringe a $G \to \varphi(G)$ e tale che $\varphi(g) \neq 1$.
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. □

1.4 Algebre su Campi e Dimensione

Ci poniamo ora l'obiettivo di studiare le algebre finitamente generate su campi. Dal Lemma di Normalizzazione di Noether, sappiamo che data una K-algebra A possiamo individuare, dall'inclusione $K \to A$, una parte trascendente su K e una parte intera. Questo ci ha permesso di definire una nozione di dimensione mediante il grado di trascendenza di A su K.

Definizione 1.40. Sia A un anello. La *dimensione di Krull* di A è

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

Chiaramente la dimensione di un anello può anche essere infinita. Questo può succedere anche nel caso noetheriano: anche se non esistono catene di lunghezza infinita può accadere che non ci sia un limite superiore alla lunghezza delle catene. Esibiremo un dominio noetheriano che ha catene di primi di lunghezza arbitraria: il controesempio di Nagata.
In termini di dimensione, i risultati sulle estensioni intere si traducono così:

Proposizione 1.41. 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:

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

Contraendo gli ideali, otteniamo una catena di primi in A e i contenimenti rimangono stretti per il Corollario 1.12, da cui $\dim(A) \geq n = \dim(B)$. L'altra disuguaglianza è una conseguenza diretta del Teorema del Going Up. □

Per le $\mathbb{K}$-algebre che sono anche domini, abbiamo allora definito due nozioni: il grado di trascendenza su $\mathbb{K}$ e la dimensione di Krull. In realtà questi coincidono; mostriamolo dapprima per gli anelli di polinomi.

Teorema 1.42. Sia $A = \mathbb{K}[X_1, \ldots, X_n]$ l'anello di polinomi su $\mathbb{K}$ in n variabili. Allora $\operatorname{tr}_{\deg} A = \dim A$.

Dimostrazione. Chiaramente $\operatorname{tr}_{\deg} A = n$. Mostriamo che $\dim A = n$. Procediamo per induzione sul numero di variabili. Se $n = 1$, $\mathbb{K}[X]$ è un PID e quindi ha dimensione 1. Procediamo al passo induttivo. Una catena di primi è

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

e quindi $\dim A \geq n$. Mostriamo l'altra disuguaglianza. Supponiamo di avere una catena di primi

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

e mostriamo che $m \leq n$. Sia $0 \neq f \in \mathfrak{p}_1$ irriducibile[6]. Quozientiamo $\mathbb{K}[X_1, \ldots, X_n]/(f) = B$ ottenendo

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

[6] Possiamo supporre che f sia irriducibile poiché, dato che A è un UFD, ogni elemento ammette una fattorizzazione in irriducibili $p = \prod p_i^{\alpha_i}$. Per primalità dell'ideale, uno dei fattori primi deve appartenere a $\mathfrak{p}_1$ e possiamo prendere come f uno d i questi fattori.

Notiamo che siamo una $\mathbb{K}$-algebra finitamente generata, quindi per il Lemma di Normalizzazione di Noether esistono $Y_1, \ldots, Y_r$ algebricamente indipendenti tali che B è intero su $\mathbb{K}[Y_1, \ldots, Y_r]$. Poiché (f) è una relazione tra i generatori, per l'Osservazione 1.29, $r < n$. Per il Corollario 1.12, la catena di primi $\mathfrak{p}_i/(f)$ dà una catena di $m-1$ primi distinti $\mathfrak{p}_i/(f) \cap \mathbb{K}[Y_1, \ldots, Y_r]$. Per ipotesi induttiva, $\mathbb{K}[Y_1, \ldots, Y_r]$ ha dimensione $r < n$; B ha la stessa dimensione di $\mathbb{K}[Y_1, \ldots, Y_r]$ e dunque $m - 1 \leq r < n$, cioè $m \leq n$. □

Mostriamo ora che la stessa proprietà può essere estesa ai domini che sono $\mathbb{K}$-algebre finitamente generate:

Teorema 1.43. Sia A una $\mathbb{K}$-algebra finitamente generata che è un dominio. Allora $\operatorname{tr}_{\deg} A = \dim A$.

Dimostrazione. Per il Lemma di Normalizzazione di Noether, A è intero su $\mathbb{K}[Y_1, \ldots, Y_r]$, e dunque $\operatorname{tr}_{\deg} A = r$. D'altronde la dimensione di Krull di un anello A è uguale alla dimensione di Krull di una qualsiasi sua estensione intera B, da cui l'uguaglianza cercata. □

Abbiamo visto che per algebre finitamente generate che sono anche domini il grado di trascendenza e la dimensione di Krull coincidono. Cosa ci facciamo con la dimensione? Ad esempio potrebbe essere uno strumento utile per condurre dimostrazioni per induzione. Intuitivamente quozientare dovrebbe far calare la dimensione, e prestarsi come passo induttivo. Effettivamente questo accade spesso: cerchiamo di formalizzare questo concetto.

Definizione 1.44. 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 *profondità* di $\mathfrak{p}$ è la dimensione di $A/\mathfrak{p}$, e si denota con $\operatorname{depth}(\mathfrak{p})$.

Proposizione 1.45. Sia $S = \mathbb{K}[x_1, \ldots, x_m]$ un dominio con $\dim S = n$ e sia $\mathfrak{p}$ un primo di altezza 1. Allora $\dim S/\mathfrak{p} = n - 1$.

Dimostrazione. Studiamo prima il caso in cui $S = \mathbb{K}[X_1, \ldots, X_n]$ è un anello di polinomi. 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

$$f = f_r(x_2, \ldots, x_m)x_1^r + \ldots + f_0(x_2, \ldots, x_m)$$

e notiamo che $\mathbb{K}[x_2, \ldots, x_n] \cap (f) = \{0\}$. Dato che (f) è il nucleo della proiezione al quoziente in $S/(f) = S/\mathfrak{p}$, $\mathbb{K}[x_2, \ldots, x_n]$ si immerge in $S/\mathfrak{p}$, e indichiamo la sua immagine con $\mathbb{K}[\bar{x}_2, \ldots, \bar{x}_n]$. Per il Lemma di Normalizzazione di Noether e l'Osservazione 1.29 si ha dunque $\dim S/\mathfrak{p} < n$. D'altra parte qui abbiamo almeno $n-1$ elementi algebricamente indipendenti, gli $\bar{x}_2, \ldots, \bar{x}_n$, e dunque $\dim S/\mathfrak{p} = n - 1$.

Affrontiamo ora il caso generale, e supponiamo che S sia intero su $\mathbb{K}[Y_1, \dots, Y_r]$. Notiamo intanto che deve essere $r = n$ perché le estensioni intere preservano la dimensione. Se $\mathfrak{p} \in \operatorname{Spec} S$ denotiamo $\mathfrak{p}_0 = \mathfrak{p} \cap \mathbb{K}[Y_1, \dots, Y_r]$. Mostriamo che $\operatorname{ht}(\mathfrak{p}_0) = 1$. L'altezza di $\mathfrak{p}_0$ non può essere 0 perchè se in S avremmo allora 2 primi distinti contenuti l'uno nell'altro che si contraggono allo stesso ideale; questo è assurdo per il teorema 1.12. Per il Teorema del Going Down, l'altezza non può essere maggiore di 1 perchè in tal caso si negherebbe il fatto che $\mathfrak{p}$ abbia altezza 1. Abbiamo che $S/\mathfrak{p}$ è intero su $\mathbb{K}[Y_1, \dots, Y_r]/\mathfrak{p}_0$, e quindi ha la stessa dimensione, che è $n-1$. □

Definizione 1.46. 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 1.47. 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

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

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. Quindi

$$r = \dim S/\mathfrak{p} - \dim S/\mathfrak{p}' = \operatorname{depth}(\mathfrak{p}) - \operatorname{depth}(\mathfrak{p}')$$

□

Corollario 1.48. Se S è anche un dominio gli ideali massimali hanno tutti la stessa altezza.

Dimostrazione. Se S è un dominio, (0) è un ideale primo. Dalla relazione

$$r = \dim S/\mathfrak{p} - \dim S/\mathfrak{p}'$$

scelto $p = (0)$ e p' un qualsiasi ideale massimale, si ottiene

$$r = \dim S - \dim S/\mathfrak{p}'$$

$S/\mathfrak{p}'$ è un campo, e quindi ha dimensione 0. Per ogni massimale, $r = \dim S$, da cui la tesi. □

In geometria algebrica, questi teoremi hanno come conseguenza che se l'anello coordinato è un dominio, cioè la varietà è irriducibile, non vi sono punti di dimensione diversa. Vediamo ora che se S non è un dominio possono presentarsi alcuni problemi:

Controesempio 1.49. Consideriamo in $S = \mathbb{K} \times \mathbb{K}[X_1, \ldots, X_n]$ gli ideali massimali $\mathfrak{m}_1 = 0 \times \mathbb{K}[X_1, \ldots, X_n]$ e $\mathfrak{m}_2 = \mathbb{K} \times (X_1, \ldots, X_n)$. È chiaro che $0 = \mathrm{ht}(\mathfrak{m}_1) \neq \mathrm{ht}(\mathfrak{m}_2) = n$.

Esercizio 1.50. Sia $R = \mathbb{K}[X] \times \mathbb{K}[Y]$. Calcolarne la dimensione di Krull e dire se esiste un insieme algebricamente indipendente di cardinalità 2.

Soluzione. Ricordiamo che gli ideali di un prodotto sono i prodotti degli ideali dei fattori. Di conseguenza, dato che un prodotto di anelli non nulli non è mai un dominio, la dimensione di Krull di un prodotto è pari al massimo delle dimensioni dei fattori. Dunque $\dim(R) = 1$.
Inoltre, non esistono insiemi algebricamente indipendenti di due elementi. Infatti, siano $A = (p_1(X), p_2(Y))$ e $B = (q_1(X), q_2(Y))$ due elementi di un insieme algebricamente indipendente. Allora, dato che $\mathbb{K}[X]$ ha grado di trascendenza 1, si ha che $\{p_1(X), q_1(X)\}$ sono algebricamente dipendenti visti come elementi di $\mathbb{K}[X]$. Di conseguenza esiste un polinomio $f_1(x, y)$ tale che $f_1(p_1(X), q_1(X)) = 0$. Allo stesso modo, esiste f_2 tale che $f_2(p_2(Y), q_2(Y)) = 0$. Di conseguenza, $f_1(A, B)f_2(A, B) = 0$, negando l'indipendenza. □

Esempio 1.51. Sia R l'anello locale $\mathbb{Z}_{(p)}$, con p primo, e consideriamo $\frac{p}{1} = t$ il generatore dell'ideale massimale di R. Consideriamo gli ideali di $R[X]$ $\mathfrak{m}_1 = (tX - 1)$ e $\mathfrak{m}_2 = (t, X)$. Mostrare che sono massimali e che hanno altezzze diverse.

Gli ideali sono massimali perché i quozienti sono campi. Questi due massimali hanno altezze diverse: infatti $\mathrm{ht}(\mathfrak{m}_1) = 1$, perché $\mathfrak{m}_1$ è generato da un solo elemento, e

Proposizione 1.52. 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. □

Invece $\mathrm{ht}(\mathfrak{m}_2) \geq 2$ perché abbiamo la catena $(0) \subsetneq (x) \subsetneq \mathfrak{m}_2$.[7].

Esercizio 1.53. Sia $A = \mathbb{K}[X^2, X^3]$. Dimostrare che gli ideali primi non nulli hanno altezza 1.

Soluzione. Sappiamo che in $\mathbb{K}[X]$ tutti i primi non nulli hanno altezza 1. $\mathbb{K}[X]$ è intero su A perché X soddisfa il polinomio $t^3 - X^3 \in \mathbb{K}[X^2, X^3][t]$. Di conseguenza, $\dim A = 1$ e quindi $\mathrm{ht}(\mathfrak{p}) \leq 1$ per ogni primo $\mathfrak{p}$. D'altronde, ogni primo non nullo contiene l'ideale primo 0, da cui l'uguaglianza. □

[7] In realtà è esattamente 2 per la Proposizione 3.42.

Esercizio 1.54. Determinare la chiusura integrale di $R = \mathbb{K}[X,Y]/(Y^3 - X^5)$ nel 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. Questo si può vedere via

- Forza bruta: uno lo vede come polinomio in Y, lo prova a fattorizzare e scopre che dovrebbe essere della forma $(Y - p(x))(Y^2 + \ldots)$. Dunque come polinomio in $\mathbb{K}(X)$ 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.
- Qualcosa di più raffinato.

Soluzione. Consideriamo l'omomorfismo

$$\begin{array}{rccc} \vartheta\colon & \mathbb{K}[X,Y] & \longrightarrow & \mathbb{K}[T^3,T^5] \\ & X & \longmapsto & T^3 \\ & Y & \longmapsto & T^5 \end{array}$$

Questo è chiaramente surgettivo; mostriamo che $\operatorname{Ker}(\vartheta) = (Y^3 - X^5)$. Chiaramente $\operatorname{Ker}\vartheta \supseteq (Y^3 - X^5)$. Mostriamo allora che $\operatorname{Ker}\vartheta \subseteq (Y^3 - X^5)$. 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, e sappiamo invece che ha grado di trascendenza e dunque dimensione 2.

A meno di isomorfismo possiamo quindi cercare la chiusura integrale di $\mathbb{K}[T^3,T^5]$ nel suo campo delle frazioni, cheè $\mathbb{K}(T)$, 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 $\lambda^3 - T^3$, quindi la chiusura integrale contiene $\mathbb{K}[T]$, che però è integralmente chiuso. Dunque la chiusura integrale è esattamente $\mathbb{K}[T]$. □

Esercizio 1.55. Calcolare la dimensione di $A = \mathbb{Z}[\sqrt{-3}, 1/2]$ e determinarne la chiusura integrale B in $\mathbb{Q}(\sqrt{-3})$.

Soluzione. Sia $S = \{2^n \mid n \in \mathbb{N}\}$. Chiaramente vale $A = S^{-1}\mathbb{Z}[\sqrt{-3}]$. Inoltre, $\mathbb{Z}[\sqrt{-3}] \subset B \subset \mathbb{Q}(\sqrt{-3})$. Dato che la chiusura integrale si comporta bene con le frazioni 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, quindi B è la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-3})$, che è $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ per 1.1. D'altronde

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

e concludiamo che A è integralmente chiuso in $\mathbb{Q}(\sqrt{-3})$. Per quanto detto quindi il nostro anello ha la stessa dimensione di $S^{-1}\mathbb{Z}$ per interezza dell'estensione e quindi la dimensione è 1. □

Esercizio 1.56. 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 (parziale). Mostriamo che non è un UFD mostrando che 2 è irriducibile ma non primo. Scriviamo

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

e notiamo che 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 $m, n \in \mathbb{Z}$. Se $\mathbb{N}\colon \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \to \mathbb{N}$ è la norma introdotta l'altra volta si può verificare che gli invertibili hanno norma 1, e lavorando con la norma supponendo 2 riducibile si giunge ad un assurdo. □

1.5 Anelli Artiniani

Definizione 1.57. Sia A un anello. A è artiniano se verifica la *descending chain condition* o equivalentemente se ogni famiglia di ideali (ordinata per inclusione) ha un elemento minimale.

Assumiamo i seguenti fatti sugli anelli artiniani:

Proposizione 1.58. Sia A un anello artiniano. Allora

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

L'obiettivo è quello di approfondire la conoscenza di questi anelli; in particolare, mostrare che sono tutti e soli quelli noetheriani di dimensione 0. Ricordiamo il seguente fatto, che ci sarà utile in seguito:

Proposizione 1.59. Sia A un anello noetheriano e sia I un ideale. Allora esiste $n \in \mathbb{N}$ tale che $\sqrt{I}^n \subseteq I$.

Proposizione 1.60. Sia A un anello artiniano. Allora il nilradicale $\mathcal{R}$ è nilpotente.

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

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

Chiaramente Σ è non vuoto perché $\mathcal{R} \in \Sigma$. Per artinianità, esiste allora un ideale $\mathfrak{c} \in \Sigma$ minimale per inclusione. 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 $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a} \neq 0$, quindi otteniamo $(x)\mathfrak{a} = (x)$. Esiste quindi $y \in \mathfrak{a}$ 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 $(0) \neq \mathfrak{c}\mathfrak{a} = (0)\mathfrak{a} = (0)$. □

Abbiamo necessità di un altro lemma:

Lemma 1.61. Sia A un anello e supponiamo che (0) si scriva come prodotto finito di ideali massimali (anche con ripetizione). Allora

$$A \text{ è noetheriano} \iff A \text{ è artiniano}$$

Dimostrazione. Siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ 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

$$A/\mathfrak{m}_1 \qquad \mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2 \qquad \mathfrak{m}_1\mathfrak{m}_2/\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \quad \cdots \quad \prod_{i=1}^{r-1} \mathfrak{m}_i \Big/ \prod_{i=1}^{r} \mathfrak{m}_i = \prod_{i=1}^{r-1} \mathfrak{m}_i \Big/ (0)$$

che sono spazi vettoriali 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 sono spazi vettoriali. Inoltre, i sottospazi come $A/\mathfrak{m}_i$-spazi vettoriali coincidono con i sottomoduli come A-moduli. Inoltre la a.c.c. vale per A se e solo se vale per ogni quoziente, e similmente la d.c.c. vale per A se e solo se vale per ogni quoziente. Questo si vede guardando la successione esatta

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

perché se due termini di una successione esatta sono artiniani/noetheriani, allora lo è anche il terzo. Andando a ritroso si arriva a dire che per A vale la a.c.c. La stessa cosa è vera per la d.c.c. Dunque

$$A \text{ noetheriano} \Leftrightarrow A/\prod \mathfrak{m}_i \text{ noetheriani} \Leftrightarrow A/\prod \mathfrak{m}_i \text{ artiniani} \Leftrightarrow A \text{ artiniano}$$

□

Teorema 1.62. 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 1.58. 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

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

Per il lemma, abbiamo allora che A è noetheriano, come voluto.

Mostriamo ora l'altra implicazione. Sia A noetheriano di dimensione 0. Per noetherianità, (0) ammette una decomposizione primaria: i primi associati P_i sono tutti e soli gli ideali primi di A. Se infatti esistesse un primo P diverso da questi, $P \supseteq \cap P_i$ e per il lemma di scansamento esiste i tale che $P = P_i$. Poiché A ha dimensione 0, tali primi sono anche massimali. Denotandoli con $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$, per la proposizione 1.59, otteniamo, usando che $\bigcap_{i=1}^t \mathfrak{m}_i = \mathcal{R}$,

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

e per il lemma, da A noetheriano segue A artiniano. □

1.6 Lunghezza di Moduli

Definizione 1.63. 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. Ogni catena massimale, cioè una catena nella quale M_i/M_{i+1} non ha sottomoduli non banali, è detta *serie di composizione*.

Teorema 1.64. 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 $M = M_0 \subsetneq \ldots \subsetneq M_k = 0$ una serie di composizione di lunghezza minima, e definiamo $N_i = N \cap M_i$. Otteniamo così la catena

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

che però può avere dei termini ripetuti. N_i/N_{i+1} è A-sottomodulo di M_i/M_{i+1}, che per ipotesi non ha sottomoduli propri. Se $N_i/N_{i+1} = 0$, allora $N_i = N_{i+1}$ e dunque possiamo ridurre la lunghezza della catena, altrimenti il contenimento è proprio. La serie ottenuta eliminando le ripetizioni è quindi di composizione. Dunque $\ell(N)$ è ben definito perché esiste una serie di composizione, e per quanto appena visto $\ell(N) \leq \ell(M)$. Se fosse $\ell(N) = \ell(M)$, da $M_{k-1}/0 = N_{k-1}/0$ otteniamo $N_{k-1} = M_{k-1}$. Iterando, da $M_{k-2}/M_{k-1} = N_{k-2}/N_{k-1}$, dall'uguaglianza dei moduli per cui quozientiamo e da $N_{k-2} \subseteq M_{k-2}$ otteniamo $N_{k-2} = M_{k-2}$. Si conclude allora che $M = N$, contro le ipotesi.

2. Applicando il passo precedente alla serie di composizione

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

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

3. Presa una serie di composizione di M, di lunghezza $k \leq \ell(M)$ per il passo precedente, per definizione di $\ell(M)$, che è il minimo delle lunghezze delle serie di composizione, si ha $k = \ell(M)$. Inoltre, presa una catena (M_i), se la sua lunghezza è $\ell(M)$ deve essere una serie di composizione. Comunque per il passo precedente la sua lunghezza non supera $\ell(M)$, e se è minore basta aggiungere dove possibile fino a raggiungere lunghezza $\ell(M)$.

□

Teorema 1.65. *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, 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 $M_k = 0$.

□

Ricordiamo che

Teorema 1.66. Un modulo finitamente generato su un anello artiniano (risp. noetheriano) è artiniano (risp. noetheriano).

Esempio 1.67. Dato che artiniano vuol dire noetheriano di dimensione 0, i moduli finitamente generati su un anello artiniano sono di lunghezza finita.

Proposizione 1.68. Sia $0 \to M \xrightarrow{f} N \xrightarrow{g} K \to 0$ una successione esatta di moduli che ammettono serie di composizione. Allora $\ell(N) = \ell(M) + \ell(K)$.

Dimostrazione. Sia $K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m$ una serie di composizione per K e sia $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n$ una serie di composizione per M. Consideriamo allora la catena data dalle controimmagini dei K_i in N e quella delle immagini degli M_i in N. Otteniamo così la catena

$$f(M_0) \subsetneq \dots f(M_n) = g^{-1}(K_0) \subsetneq g^{-1}(K_1) \subsetneq \cdots \subsetneq g^{-1}(K_m)$$

che è una serie di composizione per N. □

Esercizio 1.69. 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. □

Il viceversa è falso.

Controesempio 1.70. $A = \prod_{i=1}^{\infty} \mathbb{K}$, con $\mathbb{K}$ campo, non è noetheriano nemmeno a piangere, ma i suoi localizzati lo sono sempre.

Dimostrazione. Basta prendere la catena degli oggetti del tipo "le prime n coordinate sono non 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. □

Vedremo che in realtà la noetherianità è una proprietà locale se ci restringiamo a una classe buona di anelli.

Spoiler 1.71. Se ogni elemento di A è contenuto in un numero finito di ideali massimali, allora A è noetheriano se e solo se per ogni $\mathfrak{p} \in \operatorname{Spec} A$ lo è $A_\mathfrak{p}$.

Capitolo 2

Moduli Graduati e Completamenti

2.1 Anelli e Moduli Graduati

Definizione 2.1. Un *anello graduato* è un gruppo abeliano della forma

$$R = \bigoplus_{n=0}^{\infty} R_i$$

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

Esempio 2.2. Gli anelli di polinomi, dove R_j sono i polinomi omogenei di grado esattamente j più lo 0.

Osservazione 2.3. R_0 è un sottoanello, gli altri R_i sono in generale solo sottogruppi.

Definizione 2.4. Un elemento di un anello graduato si dice *omogeneo* se appartiene a uno degli R_j. Per gli elementi omogenei è ben definito il loro grado, che è j. Per convenzione, il grado di 0 è -1. Usando questa convenzione denotiamo $A_{-1} = (0)$.

Definizione 2.5. Un *R-modulo graduato* su anello graduato R è un R-modulo che si scrive come somma di gruppi abeliani

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

dove R agisce in modo che

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

Osservazione 2.6. Ogni M_n è un R_0-modulo.

Teorema 2.7. Sia $A = \bigoplus_{n=0}^{\infty} A_n$ un anello graduato noetheriano. A è generato come A_0-algebra da $x_1, \ldots, x_s$ 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 per noetherianità (come A-modulo) da $y_1, \ldots, y_s$, che possiamo supporre omogenei[1]. Definiamo la A_0-algebra $A' = A_0[y_1, \ldots, y_s]$ 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 $\bigoplus_{n=1}^{\infty} A_n$, possiamo scrivere per ipotesi

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

Poiché y è omogeneo di grado n e gli y_i sono omogenei di grado k_i, possiamo supporre che ogni a_i sia omogeneo di grado $n - k_i$; per motivi di grado, infatti, tutti gli elementi omogenei della somma di grado diverso da n devono cancellarsi. Per ipotesi induttiva allora, $a_i \in A_0[y_1, \ldots, y_r]$, e quindi $y \in A_0[y_1, \ldots, y_s]$. □

Osservazione 2.8. Se A è un anello graduato noetheriano, anche A_0 è un anello noetheriano, in quanto si scrive come $A/\bigoplus_{n=1}^{\infty} A_n$. Grazie a questa osservazione, possiamo concludere che se A_0 è noetheriano allora anche $A = A_0[x_1, \ldots, x_n]$ è noetheriano, per 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. Allora M è generato da un numero finito di elementi omogenei $m_1, \ldots, m_t$ con $\deg m_j = r_j$. Come mostrato in precedenza nel caso di anelli, possiamo infatti scrivere ogni $x \in M_n$ come

$$x = \sum_{J} f_J(x) m_J$$

dove $f_J(x)$ è omogeneo di grado $n - r_J$. Di conseguenza, M_n è finitamente generato come A_0-modulo dagli elementi della forma $g_J(x)m_J$, con g_J un monomio nei generatori $x_1, \ldots, x_s$ del Teorema precedente di grado $n - r_J$.

Osservazione 2.9. Abbiamo visto che i moduli per cui si la lunghezza è ben definita sono quelli che sono contemporaneamente noetheriani e artiniani. Se A_0 è artiniano, è allora ben definita la lunghezza di M_n come A_0-modulo.

[1] A meno di spezzare in componenti omogenee.

2.2 Completamenti

Definizione 2.10. 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*

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

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

Osservazione 2.11. 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.

Notazione 2.12. Sia R un anello e I un ideale. Consideriamo la filtrazione

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

cioè data da $m_i = I^i$. Indichiamo tale completamento con $\hat{R}_I$.

Esempio 2.13. Consideriamo l'anello $R = S[x_1, \ldots, x_n]$ e consideriamo l'ideale massimale $m = (x_1, \ldots, x_n)$. Un elemento di $\hat{R}_m$ è della forma $(g_1, g_2, \ldots, g_n, \ldots)$, dove $g_1 \in R/m \cong S$. Invece g_2 è un elemento della forma $[a_0 + a_1 x] \pmod{m^2}$. La condizione di compatibilità dice che g_1 è $[a_0] \pmod{m}$, e analogamente $g_3 = [a_0 + a_1 x + a_2 x^2] \pmod{m^3}$, $g_4 = [a_0 + a_1 x + a_2 x^2 + a_3 x^3] \pmod{m^4}$. È immediato a questo punto mostrare che $\hat{R}_m \cong S[[x_1, \ldots, x_n]]$.

Esempio 2.14. 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

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

Un'altra notazione possibile è

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

Per vedere come funzionano le operazioni scriviamone un altro

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

Sommandoli otteniamo

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

La differenza sostanziale è che con la prima notazione non c'è bisogno di riporti, con la seconda sì.

Esempio 2.15. Verificare che in $\widehat{\mathbb{Z}}_{(p)}$ si ha $1 + 2 + 4 + 8 + \ldots = -1$, dove $-1 = ([-1], [-1], [-1], \ldots)$.

Sia I un ideale di R e consideriamo[2] 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 2.16. Una *successione di Cauchy* $\{x_n\}$ in R è una successione tale che per ogni I^j esiste s tale che definitivamente $x_\mu - x_\nu \in I^j$. Due successioni di Cauchy $\{x_n\}$ e $\{y_n\}$ sono equivalenti se $\lim_{n\to\infty}(x_n - y_n) = 0$.

Consideriamo il completamento topologico $\tilde{R}$ delle successioni di Cauchy modulo equivalenza. Dato che le successioni si possono sommare e moltiplicare termine a termine[3], $\tilde{R}$ può essere munito di una struttura di anello. La cosa interessante è che

Teorema 2.17. Gli anelli $\hat{R}$ e $\tilde{R}$ sono isomorfi.

Dimostrazione. Data una successione $\{x_n\}$ di Cauchy esiste s tale che definitivamente $x_\mu - x_\nu \in m_j$. Dunque la proiezione su R/m_j è definitivamente costante: definiamo in tal modo g_j. È chiaro che questo non dipende dalla scelta del rappresentante per $\{x_n\}$. □

Vediamo qualche proprietà topologica di R.

Proposizione 2.18. Sia $\mathfrak{m} \in \mathrm{SpecMax}(R)$. 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. Bisogna cioè mostrare che $g_i\varphi_{j,i}(g_j^{-1}) \equiv 1 \pmod{\mathfrak{m}^i}$. Questo è vero perché $\varphi_{j,i}(g_j)\varphi_{j,i}(g_j^{-1}) \equiv 1 \pmod{\mathfrak{m}^i}$. □

Proposizione 2.19. 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.

[2] Funzionerebbe tutto anche con una filtrazione qualsiasi, ma il caso più comune è quello con $m_i = I^i$ e quindi enunciamo quasi tutto in questo caso.

[3] Andrebbe verificata la buona definizione.

Dimostrazione. Preliminarmente studiamo la chiusura dello 0. Abbiamo $a \in \overline{\{0\}}$ se e solo se per ogni j abbiamo $0 \in a + I^j$, se e solo se per ogni j abbiamo $-a \in I^j$, cioè $a \in \bigcap_j I^j$. Dunque $\overline{\{0\}} = \bigcap_j I^j$. Quindi se $\bigcap I^j = \{0\}$ allora $\{0\}$ è chiuso[4]. Allora $\Delta = \{(x, x) \in R \times R\}$ è chiusa in $R \times R$ perché è la controimmagine di 0 secondo la somma, che è continua. Avere la diagonale chiusa nel prodotto è equivalente ad essere di Hausdorff.

Viceversa se R è di Hausorff tutti i punti sono chiusi, e in particolare lo è $\{0\}$. Inoltre 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 $\bigcap I^j$. □

Definizione 2.20. 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 già 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 dentro $\hat{R}_I$ consideriamo gli ideali $\hat{I}_n$ dato dalle liste che iniziano con n zeri. Si ha

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

Enunciamo e dimostriamo ora un caso particolare del Teorema di Intersezione di Krull:

Teorema 2.21 (di Intersezione di Krull)**.** Siano I un ideale di un anello R noetheriano. Allora esiste $r \in I$ tale che $(1 + r)(\bigcap_j I^j) = \{0\}$.

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

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

dove la $\subseteq$ segue da quanto detto e la $\supseteq$ segue scrivendo $x = rx = r^2x = r^3x = \ldots$. Dato che R è noetheriano $\bigcap I^j$ è finitamente generato da $x_1, \ldots, x_n$, ognuno col suo $(1 - r_i)$, 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 $P_n(t_1, \ldots, t_r) =\in R[t_1, \ldots, t_r]$[5] tale che $x = P_n(b_1, \ldots, b_r)$. 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

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

[4] E similmente lo sono tutti i punti.

[5] "E ad essere sincero dovrei chiamare queste t come T maiuscole, perché s'era detto... ma vabbè.

si stabilizza ad un certo N, e quindi possiamo scrivere

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

dove i Q_i sono omogenei[6] 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. □

Corollario 2.22. Sia R un anello noetheriano e I un ideale di R. Se R è un dominio oppure è locale allora $\bigcap_j I^j = \{0\}$.

Corollario 2.23. Se R è un dominio noetheriano o un anello noetheriano locale la topologia I-adica è di Hausdorff.

Esercizio 2.24. $\widehat{\mathbb{Z}}_{(10)}$ non è un dominio perché si scrive come $\widehat{\mathbb{Z}}_{(2)} \oplus \widehat{\mathbb{Z}}_{(5)}$.

Soluzione. Per il Teorema Cinese del Resto, 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. □

In alcuni anelli non funziona nemmeno per I massimale. Comunque 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 2.25. 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 $6^{5^{i-1}}$ funziona. □

2.3 Il Lemma di Artin-Rees

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

Definizione 2.26. Una filtrazione del tipo

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

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

[6] Trucchi soliti.

Definizione 2.27. Sia M un R-modulo e I un ideale. Una filtrazione di M è una *I-filtrazione*

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

se per ogni $n \geq 0$ $IM_n \subseteq M_{n+1}$. Se definitivamente vale $IM_n = M_{n+1}$ diciamo che la I-filtrazione è *I-stabile*.

L'esempio più semplice è dato dalla filtrazione

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

che è I-stabile per definizione.

Definizione 2.28. Dato R anello e I ideale definiamo il *blow up di I in R* come l'anello graduato

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

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

$$B_J M = M_0 \oplus M_1 \oplus \ldots \oplus M_n \oplus \ldots$$

è un $B_I R$-modulo graduato.

Proposizione 2.29. 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.

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 M_n[7], ovvero $M_{n+1} = I^i M_n$, per cui J è I-stabile.

Viceversa se J è I-stabile, esiste $n \in \mathbb{N}$ tale che per ogni $m \geq n$ vale $M_{m+1} = IM_m$. Allora $B_J M$ è generato come $B_I R$-modulo dai generatori (finiti per ipotesi) di $M_0, \ldots, M_n$. □

Lemma 2.30 (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.

[7] 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 I prima o poi da M_n bisogna passarci.

Dimostrazione. Denotiamo le filtrazioni con J e J', chiamiamo $M'_i = M' \cap M_i$; notiamo subito che $B_{J'}M'$ è un B_IR-sottomodulo graduato di B_JM. Dato che J è I-stabile, per la Proposizione precedente B_JM è un B_IR-modulo finitamente generato. Ma B_IR è una R-algebra finitamente generata perché R è noetheriano e possiamo pensarla come algebra polinomiale $R[g_1, \ldots, g_k]$, dove $g_1, \ldots, g_k$ sono generatori di I. Per il Teorema della Base di Hilbert, B_IR è un anello noetheriano. Allora B_JM è un B_IR-modulo noetheriano, e B'_JM' in quanto suo sottomodulo deve essere finitamente generato. Per la Proposizione possiamo concludere che J' è I-stabile. □

Possiamo ora dimostrare il Teorema di Intersezione di Krull nella sua forma più generale:

Teorema 2.31 (di Intersezione di Krull)**.** Siano I un ideale di un anello R noetheriano e sia M un R-modulo finitamente generato. Allora esiste $r \in I$ tale che $(1 + r)(\bigcap_j I^j M) = (0)$.

Dimostrazione. Sia $M' = \bigcap_j I^j M$. 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; dunque esiste p tale che $M' \cap I^{p+1}M = I(M' \cap I^p M)$. Di conseguenza,

$$\begin{aligned} M' =& \bigcap I^j M \\ =& \bigcap (I^j M \cap I^{p+1} M) \\ =& \left(\bigcap I^j M\right) \cap I^{p+1} M \\ =& M' \cap I^{p+1} M \\ =& I(M' \cap I^p M) \\ =& IM' \end{aligned}$$

e per Nakayama esiste $r \in I$ tale che $(1 + r)M' = 0$. □

A prima vista, si potrebbe pensare che questo valga in generale, senza bisogno del Lemma di Artin-Rees, utilizzando la formula

$$I(\bigcap_j I^j M) = \bigcap_j I^j M$$

In realtà questa è falsa. Consideriamo l'anello $\mathbb{Z}[x, y_1, y_2, \ldots, y_n, \ldots]$ quozientato per l'ideale J delle relazioni

$$px = 0$$
$$x = py_1 = p^2 y_2 = \ldots = p^n y_n = \ldots$$
$$x^2 = xy_j = y_i y_j = y_i^2 = 0$$

Sia $I = (p)$. Se $\bigcap I^j = (x)$, allora

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

e avremmo quindi un controesempio all'uguaglianza data sopra. Mostriamo allora che $\bigcap I_j = (x)$. Sicuramente vale $x \in \bigcap I^j$ e dunque un'inclusione. Mostriamo l'altra. Abbiamo $\bigcap I_j \subseteq \langle x, y_1, y_2, \ldots, y_n, \ldots\rangle_{\mathbb{Z}}$, cioè non ci sono costanti. Consideriamo

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

Scegliamo $t > m$ e leggiamo tutto in $\mathbb{Z}[x, y_1, y_2, \ldots, y_n, \ldots]$ (prima di quozientare). Abbiamo

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

Questo crea problemi: focalizzando l'attenzione 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 $\alpha x + \alpha_1 y_1 + \alpha_2 y_2 + \ldots + \alpha_m y_m \in (x)$. Dunque $\bigcap I^j \subseteq x$, e abbiamo già mostrato l'altra inclusione. Notiamo che abbiamo incidentalmente mostrato che le ipotesi di Krull sono necessarie. Infatti comunque scelto $r \in I = (p)$ abbiamo $(1 + r)(x) = (x)$.

Proposizione 2.32. Se $\{M_n\}$ e $\{\bar{M}_n\}$ sono filtrazioni I-stabili di un modulo M, allora hanno "differenze limitate", cioè esiste n_0 tale che per ogni n vale sia $M_{n+n_0} \subseteq \bar{M}_n$ che $\bar{M}_{n+n_0} \subset M_n$. 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. Dato che $IM_n \subseteq M_{n+1}$ vale $I^n M \subset M_n$, quindi $I^{n+n_0} M \subset M_n$. Viceversa poiché per ogni $n \geq n_0$ vale $IM_n = M_{n+1}$ abbiamo $M_{n+n_0} = I^n M_{n_0} \subset I^n M$. □

Teorema 2.33 (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.

In altre parole la I-topologia sulla sottovarietà coincide con quella indotta come sottovarietà di M.

Forniamo ora un controesempio al Lemma di Artin-Rees. Quello che vedremo è che esistono moduli $M' \subseteq M$ tali che la I-topologia su M' considerato come modulo a sé stante non coincide con topologia indotta come sottospazio dalla I-topologia di M.
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 leggiamo A come sottomodulo di B.
Consideriamo il completamento $\hat{A}_{(p)}$ rispetto alla topologia indotta dall'ideale (p), che è per definizione

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

perché $pA = 0$. 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 aperto di base $\alpha(A) \cap p^k B$. Ricordiamo che

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

ed è allora facile vedere che

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

Scriviamo la filtrazione $\mathcal{F}$ di $\alpha(A) \cong A$. Questa è fatta così:

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

Il completamento di A rispetto alla topologia indotta dalla (p)-topologia di B è

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

e la mappa è quella che "dimentica le ultime coordinate", quindi è compatibile e quello 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 $\bigoplus(\ldots)$ e $\prod(\ldots)$ non sono isomorfi[8], e quindi le topologie che li inducono non possono coincidere.

2.4 Successioni Esatte e Sollevamento Henseliano

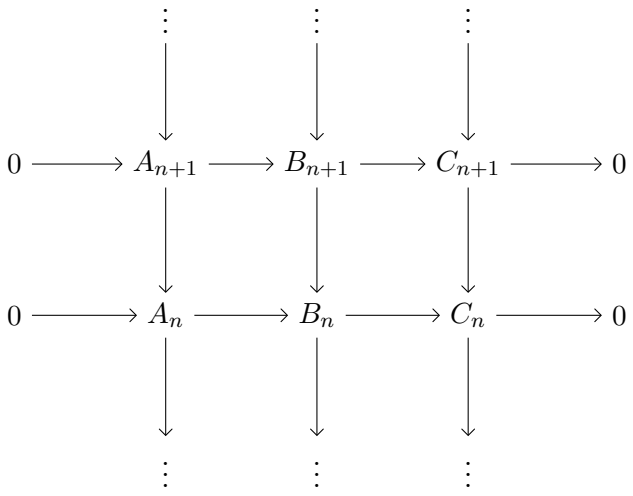
È naturale chiedersi se l'esattezza di una famiglia di successioni esatte passi al completamento.

Proposizione 2.34. 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

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

Per arrivarci ci servono un po' di risultati.

Proposizione 2.35. Sia $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ una successione esatta di sistemi inversi di R-moduli.



[8] Ad esempio per motivi di cardinalità.

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

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

Dimostrazione. Siano $A = \prod A_n$, $B = \prod B_n$ e $C = \prod C_n$. Definiamo $d^A \colon A \to A$ componente su componente $a_n \mapsto a_n - \vartheta_{n+1}(a_{n+1})$, e analogamente d^B e d^C. Il diagramma

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

commuta. Una volta definite le d basta applicare il Lemma del Serpente. Per vedere che d^A è surgettiva, sotto le ipotesi aggiuntive, bisogna soddisfare le equazioni

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

Ma questo è possibile induttivamente trovando ogni volta x_n grazie alla surgettività di ϑ_2. □

Corollario 2.36. Sia $0 \to M' \to M \to M'' \to 0$ una successione esatta di R-moduli. Sia M munito della topologia $\{M_n\}$, M' munito della topologia $\{M_n \cap M'\}$ e M'' munito della $\{\pi(M_n)\}$. Allora è esatta

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

Dimostrazione. Basta applicare la Proposizione precedente a

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

dato che le ϑ_i sono tutte surgettive perché proiezioni al quoziente. Basta allora passare ai limiti inversi.è □

Ora abbiamo gli strumenti per affrontare la

Dimostrazione della Proposizione 2.34. Per il Corollario precedente usato su $\{I^j M\}$, notando che per il membro a destra

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

e usando Artin-Rees sul membro a sinistra. □

Esercizio 2.37. 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 la topologia $\widehat{A}_{\{xA \cap I^j\}}$. Tuttavia in generale questa potrebbe essere diversa da $\widehat{A}_I$. Se aggiungiamo l'ipotesi che A sia noetheriano, però, tutto funziona perché possiamo usare la Proposizione 2.34 e la mappa $\cdot x$, passando ai completamenti, rimane iniettiva (la mappa "passata" sarebbe $\cdot \hat{x}$, dove $\hat{x} = (x, x, x, \ldots)$. Notiamo che serve passare dalla Proposizione 2.34, e non basta il Corollario, perché altrimenti a sinistra sarebbe uscito fuori $\widehat{A}_{\{I^j \cap A\}}$. Il punto è che nel Corollario abbiamo letto M' direttamente dentro M, nel senso che abbiamo considerato $\{M' \cap i^{-1}(M_n)\}$. □

Questo non vuol dire che A dominio implica $\widehat{A}_I$ dominio, anzi abbiamo già visto che è falso.

Occupiamoci ora del Teorema di Sollevamento di Hensel. Questo teorema è noto sopratutto per il suo utilizzo in campo computazionale per la fattorizzazione di polinomi in $\mathbb{Z}$. Supponiamo infatti di voler fattorizzare un polinomio $F \in \mathbb{Z}[x]$. È possibile disporre di stime sul modulo dei coefficienti dei divisori di un polinomio; il bound è chiaramente largo, ma permette, se $F = GH$, di predire che i coefficienti di G sono minori in modulo di un certo M. Supponiamo di trovare una fattorizzazione $f \equiv gh \pmod{M}$ con g di grado r. Scegliamo un rappresentante di g con i coefficienti in modulo minori di $\frac{M}{2}$. Allora 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 $\mathbb{Z}[x]$. Queste idee si trasferiscono in anelli completi:

Lemma 2.38 (di Hensel)**.** Sia R un anello locale completo. Siano poi $K = R/\mathfrak{m}$ il suo campo residuo e $F \in R[X]$ un polinomio monico che si fattorizza come[9] $f = gh$ in $K[X]$, cioè $f \equiv gh \pmod{\mathfrak{m}}$, 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.

Dimostrazione. Mostreremo solo l'esistenza.
Siano G_1 e H_1 monici tali che $g_1 \equiv g \pmod{\mathfrak{m}}$ e $h_1 \equiv h \pmod{\mathfrak{m}}$. Inoltre chiediamo che $\deg G_1 = \deg g_1$ e $\deg H_1 = \deg h_1$. Per opportuni $A_i \in \mathfrak{m}$ e

[9] In questa dimostrazione, useremo le lettere maiuscole per indicare elementi di $R[X]$ e le r ispettive minuscole per indicare le classi di resto modulo $\mathfrak{m}$.

$J_i \in R[X]$ in $R[X]$ vale

$$F - GH = \sum A_i J_i$$

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

$$j_i = gu_i + hv_i$$

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[10]

$$\deg(hv_i) = \deg(j_i - gu_i) < \deg f$$

Allora $\deg v_i < \deg g$. Scegliamo U_i e V_i con $\deg U_i = \deg u_i$ e $\deg V_i = \deg v_i$. 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

$$F - G_2 H_2 = F - G_1 H_1 - \sum A_i (\underbrace{H_1 V_i + G_1 U_i}_{=J_1 + \Gamma}) - \sum A_i A_j U_i V_j$$

dove $\Gamma \in \mathfrak{m}[x]$, dato che J_1 è il sollevato di $j_i = hv_i + gu_i$. Ne deduciamo che quanto sopra è uguale a

$$\underbrace{F - G_1 H_1 - \sum A_i J_i}_{=0} - \sum A_i \Gamma_i - \sum A_i A_j U_i V_j$$

e quindi $F \equiv G_2 H_2 \pmod{\mathfrak{m}^2}$. Ora G_2 e H_2 sono monici perché $\deg V_i < \deg G_1$ e $\deg U_i < \deg H_1$. In altre parole 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 $G_i H_i \equiv F \pmod{\mathfrak{m}^i}$. Per la completezza di R la successione coefficiente per coefficiente $G_1^k, G_2^k, \ldots$ è di Cauchy e quindi ha un limite G^k, e questo è come costruiamo G e H. Vediamo se vanno bene. Monici lo sono, ma $GH \stackrel{?}{=} F$. Basta ragionare per intorni come in analisi: fissiamo $\mathfrak{m}^s$. Definitivamente $G_n - G \in \mathfrak{m}^s$ e $H_n - H \in \mathfrak{m}^s$. 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 $F - GH = 0$. □

Non abbiamo usato l'ipotesi di località, ma è gratis dalla Proposizione 2.18.

Esempio 2.39. In $\widehat{\mathbb{Z}}_{(5)}$ prendiamo $F = x^2 + 1$ e ci chiediamo se ha radici in $\widehat{\mathbb{F}_{(5)}}$.

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

Abbiamo

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

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

Si ha $f(x) = x^2 - 1$ in $\mathbb{C}[x]$ e $x^2 - 1 = (x - 1)(x + 1)$. Dunque solleando troviamo $\alpha(z)$, $\beta(z)$ radici quadrate di $1 + z$ in $\mathbb{C}[[z]]$.

Esercizio 2.41. Sia A completo rispetto ad un ideale massimale $\mathfrak{m}$ (in particolare A è locale). Sia U il sottogruppo $1 + \mathfrak{m}$ di A^*. Sia infine n un intero positivo primo con la caratteristica di A/m (se $\operatorname{char} A/m = 0$ va bene qualunque n). 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 $x^n \equiv 1 \pmod{\mathfrak{m}}$, 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 è 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 $\alpha^n = u$. Dato che $\alpha \equiv 1 \pmod{\mathfrak{m}}$, allora $\alpha \in U$.

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 dunque $na \equiv 0 \pmod{\mathfrak{m}^2}$. Tuttavia in $A/\mathfrak{m}$ l'elemento n è invertibile perché è primo con la caratteristica e dunque possiamo scrivere $nk = 1 + m_1$ e avere $kna \equiv 0 \pmod{\mathfrak{m}^2}$, da cui $(1 + m_1)a \equiv 0 \pmod{\mathfrak{m}^2}$ e dunque $a \equiv 0 \pmod{\mathfrak{m}^2}$. 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 A è completo e si inietta in sé stesso. □

Capitolo 3

Teoria della Dimensione

La nozione di dimensione di Krull fornisce molte informazioni sull'anello; purtroppo non è semplice calcolarla. Diamo allora alcune definizioni diverse; mostreremo poi che coincidono. Le caratterizzazioni forniranno metodi più semplici per il calcolo della dimensione di un anello. Studieremo queste nozioni su anelli locali per questioni geometriche, dato che la dimensione è una nozione locale.

3.1 Funzione di Hilbert

In tutta questa sezione, se A è un anello locale il suo ideale massimale sarà $\mathfrak{m}$.

Definizione 3.1. Sia C una classe di A-moduli e sia G un gruppo abeliano. Una funzione $\lambda\colon C \to G$ viene detta *additiva* se per ogni successione esatta

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

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

Lemma 3.2. Sia λ una funzione additiva e sia

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

una successione esatta. Allora

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

Dimostrazione. Per induzione sulla lunghezza della successione esatta. Per una successione esatta corta, la tesi è vera per definizione. Supponiamo quindi di avere una successione lunga n e supponiamo vera la tesi per ogni successione di lunghezza $n-1$.

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & M_n & \xrightarrow{f_n} & M_{n-1} & \xrightarrow{f_{n-1}} & M_{n-2} & \xrightarrow{f_{n-2}} & \cdots & \xrightarrow{f_1} & M_0 & \xrightarrow{f_0} & 0 \\ & & & & & \searrow & & \nearrow & & & & & \\ & & & & & & \mathrm{Ker}(f_{n-2}) & & & & & & \\ & & & & & \nearrow & & \searrow & & & & & \\ & & & & 0 & & & & 0 & & & & \end{array}$$

Allora $\lambda(M_n) - \lambda(M_{n-1}) + \lambda(\mathrm{Ker}(f_{n-2})) = 0$ per definizione di funzione additiva e per ipotesi induttiva $\lambda(\mathrm{Ker}(f_{n-2})) - \sum_{i=0}^{n-2}(-1)^{n-2-i}\lambda(M_i) = 0$. Sottraendo la seconda relazione alla prima si ottiene la tesi. □

Sia ora λ una funzione additiva a valori in $\mathbb{Z}$ sulla classe di tutti gli A_0-moduli finitamente generati.

Definizione 3.3. Sia $M = \bigoplus_{n=0}^{\infty} M_n$ un A-modulo graduato. La *serie di Poincaré di M rispetto a λ* è la serie formale

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

Teorema 3.4 (Hilbert-Serre)**.** Sia $A = A_0[x_1, \ldots, x_s]$ un anello graduato noetheriano e sia M un A-modulo graduato noetheriano. Allora $P(M,t)$ è una funzione razionale della forma

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

con $f(t) \in \mathbb{Z}[t]$.

Dimostrazione. Per induzione su s, dove s è il numero di generatori di A come A_0-algebra.

Per $s = 0$ abbiamo $A = A_0$, ed M è un A_0-modulo finitamente generato da $y_1, \ldots, y_r$. Sia N il massimo dei gradi di $y_1, \ldots, y_r$. Allora si ha $M_n = 0$ per ogni $n > N$, per cui $P(M,t)$ è un polinomio.
Procediamo al passo induttivo. Per ogni $n \in \mathbb{N}$, consideriamo l'omomorfismo graduato di A-moduli

$$\begin{array}{rccc} \varphi_{x_s}\colon & M & \longrightarrow & M \\ & m & \longmapsto & x_s m \end{array}$$

e la successione esatta da lui indotta

$$0 \to \mathrm{Ker}(\varphi_{x_s}) \to M \xrightarrow{\varphi_{x_s}} M \to {}^{M}\!/_{\mathrm{Im}(\varphi_{x_s})} \to 0$$

Poniamo $K = \mathrm{Ker}(\varphi_{x_s})$ e $L = \mathrm{Coker}(\varphi_{x_s})$. Notiamo che questi sono moduli graduati perché l'omomorfismo è graduato e sono banalmente finitamente generati, perché sottomoduli e quozienti di moduli noetheriani. Per ipotesi, $A = A_0[x_1, \ldots, x_s]$; x_s annulla però sia K che L, per cui K ed L sono

finitamente generati anche come $A_0[x_1, \ldots, x_{s-1}]$-moduli. Componente per componente, abbiamo la successione:

$$0 \to K_n \to M_n \to M_{n+k_s} \to L_{n+k_s}$$

Applicando λ alla successione esatta otteniamo

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

Moltiplicando per t^{n+k_s} otteniamo

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

Sommando su tutti gli n, abbiamo

$$t^{k_s}P(K,t) - t^{k_s}P(M,t) + f_M(t) + P(M,t) - P(L,t) + f_L(t) = 0$$

dove f_M indica $\sum_{k=0}^{k_s-1}\lambda(M_k)t^k$ e f_L è $\sum_{k=0}^{k_s-1}\lambda(L_k)t^k$. Riordinando la somma,

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

Per ipotesi induttiva

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

da cui la tesi. □

Corollario 3.5. Sia A un anello graduato noetheriano e supponiamo che esistano degli elementi $y_1, \ldots, y_s$ di grado 1 tali che $A = A_0[y_1, \ldots, y_s]$. Sia M un A-modulo graduato noetheriano. Allora definitivamente $\lambda(M_n)$ è un polinomio in n a coefficienti in $\mathbb{Q}$ di grado uguale a $b-1$, dove b è l'ordine del polo di $P(M,t)$ in $t=1$.

Dimostrazione. Per il 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 $P(M,t) = g(t)/(1-t)^d$, dove d è l'ordine del polo e $g(1) \neq 0$. Sia $g(t) = \sum_{k=0}^{N} a_k t^k$; 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

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

Supponiamo allora $n \geq N$; si ottiene allora come coefficiente un polinomio in n di grado al più $d-1$. Concludiamo notando che il suo termine di grado massimo è

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

□

Queste tecniche servono in Teoria della Dimensione. Dato infatti A un anello locale noetheriano e $\mathfrak{m}$ un suo ideale massimale, definiamo l'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 M. Abbiamo $M_i = \mathfrak{m}^{i-1}/\mathfrak{m}^i$, inoltre $(\operatorname{gr}_{\mathfrak{m}} A)_0 = A/\mathfrak{m}$ è un campo e quindi $\lambda(M_i) = \dim_{A/\mathfrak{m}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i)$. Si applica allora il Corollario e

$$\lambda(M_i) = \dim_{A/\mathfrak{m}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i)$$

è definitivamente un polinomio P. Vale allora $\dim_{\text{Krull}} A = \deg P - 1$: sviluppiamo la teoria in questa direzione.

Lemma 3.6. Siano $p, f\colon \mathbb{N} \to \mathbb{Z}$ funzioni tali che $p(n+1) - p(n) = f(n)$. Allora

$$p(n) \in \mathbb{Q}[n] \iff f(n) \in \mathbb{Q}[n]$$

Se ciò accade, $\deg p = \deg f + 1$.

Dimostrazione. Una implicazione è ovvia: se infatti $p(n) \in \mathbb{Q}[n]$ allora lo è anche $f(n)$ per la relazione $p(n+1) - p(n) = f(n)$. Inoltre, nella relazione $p(n+1) - p(n)$ si cancellano i termini di testa e il grado diminuisce esattamente di 1.
Viceversa, se $f(n) \in \mathbb{Q}[n]$, per le 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. Un insieme di per i polinomi su $\mathbb{Q}$ è formata dai polinomi $\binom{x}{0}, \binom{x}{1}, \binom{x}{2}, \binom{x}{3}, \dots$ dove ad esempio

$$\binom{x}{3} = \frac{x(x-1)(x-2)}{3!}$$

Dunque basta dimostrare la tesi per i polinomi $\binom{x}{k}$. Studiamo quindi

$$\sum_{t=0}^{n-1} \binom{t}{k}$$

Mostriamo per induzione che questo è uguale a $\binom{n}{k+1}$.

Passo Base Se $n = 1$, $\binom{0}{k}$ è uguale a 0 se $k > 0$ e 1 se $k = 0$. D'altronde $\binom{1}{k+1}$ è uguale a 0 se $k > 0$ e 1 se $k = 0$, da cui l'uguaglianza in questo caso.

Passo Induttivo

$$\begin{aligned} \sum_{t=0}^{n} \binom{t}{k} &= \binom{n}{k} + \binom{n}{k+1} && \text{Dividendo la somma} \\ &= \binom{n+1}{k+1} && \text{Per la formula sui binomiali} \end{aligned}$$

Dato che $\binom{n}{k+1}$ ha grado $k+1$ in n abbiamo concluso. □

Proposizione 3.7. 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. definitivamente $\ell(M/M_n)$ è 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.

Dimostrazione.

1. Consideriamo l'anello e il modulo graduato indotti da $\mathfrak{q}$ e dalla filtrazione

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

$\operatorname{gr}(M)$ è naturalmente un $\operatorname{gr}_{\mathfrak{q}}(A)$-modulo graduato. Notiamo che $A/\mathfrak{q}$ è noetheriano e artiniano; infatti l'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

$$\mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$$

Passando ai radicali otteniamo

$$\mathfrak{m} = \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{p}} \subseteq \mathfrak{m} = \mathfrak{m}$$

dunque $A/\mathfrak{q}$ ha dimensione 0 ed è noetheriano, dunque è artiniano.

M_n/M_{n+1} è finitamente generato come $A/\mathfrak{q}$-modulo. Infatti, M_n/M_{n+1} è finitamente generato come A modulo e $\mathfrak{q} \subseteq \operatorname{Ann}(M_n/M_{n+1})$ e dunque risulta finitamente generato come $A/\mathfrak{q}$-modulo. Di conseguenza M_n/M_{n+1} è un $A/\mathfrak{q}$-modulo noetheriano e artiniano e ammette serie di composizione per il Teorema 1.65, cioè $\ell(M_n/M_{n+1}) < +\infty$. Di conseguenza, per ogni $i = 1, \dots, n-1$ esiste una serie di composizione

$$M_{i,0} = M_{i+1} \subseteq M_{i,1} \subseteq \cdots \subseteq M_{i,s_i} = M_i$$

Otteniamo così una serie di composizione per M/M_n

$$M_{1,s_1} = M_n \subseteq M_{1,n-1} \subseteq \cdots \subseteq M_{1,0} = M_{2,s_2} \subseteq \cdots \subseteq M_{n-1,s_{n-1}} = M$$

incollando le serie di composizione a disposizione.

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

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

dove $x_1, \dots, x_s$ generano $\mathfrak{q} \subseteq A$. Quindi, per il Corollario 3.5, definitivamente $\ell(M_n/M_{n+1}) = f(n)$, con f polinomio di grado $d-1$, dove d è l'ordine del polo. In particolare $d \leq s$ e dunque $\deg f \leq s-1$.
Vorremmo calcolare però $\ell(M/M_n)$; chiamiamo allora $\ell_n = \ell(M/M_n)$. Per $n \geq n_0$ abbiamo la relazione $\ell_{n+1} - \ell_n = f(n)$. Definiamo allora

$$p(n) = \begin{cases} \ell_n & \text{per } n \geq n_0 \\ \ell_{n_0} - \sum_{t=n}^{n_0-1} f(t) & \text{per } n < n_0 \end{cases}$$

e abbiamo $p(n+1) - p(n) = f(n)$ *per ogni* n, e non solo definitivamente. Per il Lemma 3.6 concludiamo che $p(n)$ è un polinomio che definitivamente vale ℓ_n di grado al più $\deg f + 1 = s - 1 + 1 = s$.

3. Sia $\{\tilde{M}_n\}$ un'altra filtrazione stabile di M; possiamo ripetere il ragionamente precedente e ottenere un altro polinomio $\tilde{g}(n)$ che è definitivamente $\ell(M/\tilde{M}_n)$. Per la Proposizione 2.32, due filtrazioni $\mathfrak{q}$-stabili hanno differenze limitate, cioè esiste n_0 tale che per ogni n $M_{n+n_0} \subseteq \tilde{M}_n$ e $\tilde{M}_{n+n_0} \subseteq M_n$. Allora per $n \gg 0$ valgono

$$\ell(M/M_{n+n_0}) = g(n+n_0) \geq \tilde{g}(n) = \ell(M/\tilde{M}_n), \qquad \tilde{g}(n+n_0) \geq g(n)$$

dunque deve essere $\deg g = \deg \tilde{g}$. Inoltre, posto A il rapporto fra i coefficienti direttori, devono valere

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

per cui $A = 1$.

□

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

Notazione/Riepilogo 3.8. Denotiamo con $\chi_{\mathfrak{q}}^M(n)$ il polinomio $g(n)$ associato alla filtrazione standard $\{\mathfrak{q}^n M\}$. Dunque per quanto visto $\chi_{\mathfrak{q}}^M(n) = \ell(M/\mathfrak{q}^n M)$. 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 $\mathfrak{q}$.

I polinomi ottenuti in questo modo forniscono alcuni invarianti, dipendenti solo dall'anello e non dagli ideali:

Proposizione 3.9. 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 dell'anello, $\mathfrak{q}$ contiene una potenza del suo radicale, cioè esiste $r \in \mathbb{N}$ tale che $\mathfrak{m}^r \subseteq \mathfrak{q}$. Allora dalla relazione $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ otteniamo

$$\mathfrak{m}^{rn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$$

Definitivamente, dato che i polinomi caratteristici sono legati alle lunghezze $\ell(A/\mathfrak{m}^{rn})$, $\ell(A/\mathfrak{q}^n)$, $\ell(A/\mathfrak{m}^n)$, si ha quindi

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

e quindi i polinomi hanno lo stesso grado nella variabile n. □

Dunque i polinomi $\chi_{\mathfrak{q}}^A$ hanno lo stesso grado al variare dell'ideale primario considerato:

Definizione 3.10. Sia A un anello locale noetheriano. Poniamo $d(A) = \deg \chi_{\mathfrak{q}}^A(n)$, con $\mathfrak{q}$ ideale $\mathfrak{m}$-primario qualsiasi.

Quanto dimostrato assicura la buona definizione. Notiamo inoltre che l'invariante $d(A)$ coincide con l'ordine del polo della serie di Hilbert di $\mathrm{gr}_{\mathfrak{m}}(A)$. Si può vedere questo ripercorrendo la dimostrazione della Proposizione 3.7.

3.2 Il Teorema della Dimensione

Mostriamo ora che la dimensione di Krull e l'ordine del polo nella serie di Hilbert del graduato coincidono. Diamo prima una terza definizione di dimensione, che mostreremo essere equivalente alle altre:

Definizione 3.11. Sia A un anello locale noetheriano. Definiamo $\delta(A)$ come il minimo numero di generatori di un ideale $\mathfrak{m}$-primario.

Dalla definizione, è chiaro che $\delta(A) \geq d(A)$. Supponiamo infatti che $\delta(A) = s$ e 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 $\bar{x}_1, \ldots, \bar{x}_s$ e per la Proposizione 3.7 il grado di $\chi_{\mathfrak{q}}^A(n)$ è $\leq s$, da cui la disuguaglianza. Vedremo che $\delta \leq \dim_{\mathrm{Krull}}$. Ora dimostriamo la disuguaglianza $\dim_{\mathrm{Krull}} \leq d(A)$. Abbiamo bisogno di un lemma preliminare:

Proposizione 3.12. Sia A un anello locale noetheriano con ideale massimale $\mathfrak{m}$ e sia $\mathfrak{q}$ un ideale $\mathfrak{m}$-primario. Sia M un A-modulo finitamente generato, $x \in A$ un elemento che non annulla alcun elemento del modulo[1] e $M' = M/xM$. Allora $\deg \chi_{\mathfrak{q}}^{M'} \leq \deg \chi_{\mathfrak{q}}^{M} - 1$.

Dimostrazione. Sia $N = xM$. Come A-modulo $N \cong M$, perché l'omomorfismo $\varphi_x \colon M \to M$ dato dalla moltiplicazione per x è iniettivo per l'ipotesi che x non annulli nessun elemento. Consideriamo la filtrazione $N_n = N \cap \mathfrak{q}^n M$ indotta da $\mathfrak{q}$ su N 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,

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0 \tag{3.1}$$

Per Artin-Rees, la N_n è una filtrazione $\mathfrak{q}$-stabile di N, che però è isomorfo a M. Per il terzo punto della Proposizione 3.7, $g(n)$ e $\chi_{\mathfrak{q}}^{M}(n)$ hanno lo stesso grado e lo stesso coefficiente direttore. Dunque nella (3.1) i coefficienti direttori si semplificano e $\deg \chi_{\mathfrak{q}}^{M'}(n) < \deg \chi_{\mathfrak{q}}^{M}(n)$. □

Corollario 3.13. Sia A un anello locale noetheriano e x non divisore di 0. Allora $d(A/(x)) \leq d(a) - 1$.

Possiamo ora dimostrare la disuguaglianza:

[1] Negli caso degli anelli, si dice divisore di 0

Teorema 3.14. $d(A) \geq \dim_{\text{Krull}}(A)$.

Dimostrazione. 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 in particolare ogni elemento è nilpotente. Poiché il nilradicale è l'intersezione di tutti i primi, si ha che $\mathfrak{m}$ è l'unico primo e $\dim(A) = 0$.
Sia ora $d > 0$ e consideriamo una catena di primi

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

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. Sia x' l'immagine di x in A'[2] ; x' non è un divisore di 0, e per il Corollario 3.13 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 $A/\mathfrak{m}$; dunque $\ell(A^n/\mathfrak{m}^n) \geq \ell(A'/\mathfrak{m}'^n)$, perché la lunghezza è una funzione additiva. Passando ai gradi dei rispettivi polinomi caratteristici abbiamo $d(A) \geq d(A')$. Riepilogando,

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

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

Questa disuguaglianza ha alcuni corollari importanti:

Corollario 3.15. Gli anelli locali noetheriani hanno dimensione di Krull finita.

Dimostrazione. L'ordine del polo nella serie di Hilbert-Poincarè è finito e maggiora la dimensione di Krull dell'anello. □

Corollario 3.16. 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 definizione, l'altezza di un ideale è la dimensione di $A_{\mathfrak{p}}$, che è un anello noetheriano locale; dunque l'altezza dell'ideale è finita. Inoltre, data una catena discendente di ideali primi

$$\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$$

possiamo localizzare per p_0 e ridurci a un anello locale noetheriano. La catena è allora stazionaria per motivi di dimensione. □

Dimostriamo ora l'ultima disuguaglianza:

[2] "Come mai non l'abbia chiamato $\bar{x}$... non v'è alcun motivo".

Teorema 3.17. Sia A un anello locale noetheriano. Allora $\dim_{\text{Krull}}(A) \geq \delta(A)$.

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 dunque l'ideale massimale è nilpotente. Dunque (0) è $\mathfrak{m}$-primario, e dato che (0) ha 0 generatori $\delta(A) = 0$.
Per $d \geq 1$ invece costruiamo $x_1, \ldots, x_d$ in modo che $\forall i \leq d$ valga la proposizione

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

Supponiamo di aver già costruito $x_1, \ldots, x_{i-1}$ per cui valga $\mathcal{P}$ e vediamo come costruire x_i. Siano $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ i primi associati all'ideale $(x_1, \ldots, x_{i-1})$ tali che $\text{ht}(\mathfrak{p}_j) = i-1$, se esistono. Dato che $i-1 < d = \dim_{\text{Krull}}(A) = \text{ht}(\mathfrak{m})$, per ogni j vale $\mathfrak{m} \supsetneq \mathfrak{p}_j$. Per il Prime Avoidance Lemma (o Lemma di Scansamento), $\mathfrak{m} \supsetneq \bigcup_{j=1}^{s} \mathfrak{p}_j$. Scegliamo dunque $x_i \in \mathfrak{m} \setminus \bigcup \mathfrak{p}_j$ e verifichiamo che valga $\mathcal{P}(i)$.
Supponiamo di avere un ideale primo $\mathfrak{q}$ che contiene $(x_1, \ldots, x_i)$. Questo conterrà un primo $\mathfrak{p}$ associato a $(x_1, \ldots, x_{i-1})$. Se $\mathfrak{p}$ è uno dei $\mathfrak{p}_j$, che ha altezza $i-1$, allora $\mathfrak{q} \supsetneq \mathfrak{p}$ ha altezza $\geq i$, perché $x_i \in \mathfrak{q} \setminus \mathfrak{p}_j$. Altrimenti, $\text{ht}(\mathfrak{p}) \geq i$, e allora $\text{ht}(\mathfrak{q}) \geq \text{ht}(\mathfrak{p}) \geq i$.
Iterando, troviamo l'ideale $J = (x_1, \ldots, x_d)$. Se I è un primo minimale che lo contiene, allora $\text{ht}(I) \geq d$, per cui $I = \mathfrak{m}$; altrimenti $d = \text{ht}(\mathfrak{m}) > \text{ht}(I) \geq d$. Dunque $\sqrt{J} = \mathfrak{m}$, perché il suo radicale è l'intersezione dei primi che lo contengono e l'unico ideale primo che contiene J è $\mathfrak{m}$. D'altronde, se la radice di un ideale è massimale, l'ideale è primario, da cui la tesi. □

Le disuguaglianze mostrate danno vita al seguente teorema:

Teorema 3.18 (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

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

Va notato che la definizione di $\delta(A)$ parla del numero minimo di generatori di un ideale $\mathfrak{m}$-primario; non sempre coincide dunque con il numero minimo di generatori di $\mathfrak{m}$. D'altronde, il numero di generatori del massimale fornisce una disuguaglianza sulla dimensione.

Ha senso chiedersi quando esiste un insieme di generatori di $\mathfrak{m}$ che realizza $\delta(A)$. Gli anelli che hanno questa proprietà si dicono *anelli locali regolari*, e geometricamente corrispondono ai punti non singolari di una varietà.

Corollario 3.19. Sia A un anello locale noetheriano. Allora $\dim(A) \leq \dim_K(\mathfrak{m}/\mathfrak{m}^2)$.

Dimostrazione. Per il Lemma di Nakayama, se $\bar{x}_1, \ldots, \bar{x}_s$ 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 3.20 (Teorema di Krull sull'Altezza degli Ideali)**.** Sia A noetheriano[3] 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 associato a $I = (x_1, \ldots, x_r)$. Localizzando per $\mathfrak{p}$, l'ideale $(x_1, \ldots, x_r)^e$ è $\mathfrak{p}^e$-primario. Dunque $r \geq \dim A_\mathfrak{p} = \mathrm{ht}(\mathfrak{p})$. □

Nell'esercizio 1.51, l'ideale in $\mathbb{Z}_{(p)}[x]$ era generato da due elementi e quindi aveva altezza esattamente 2 per quanto dimostrato ora.
Enunciamo separatamente un caso particolare per ragioni di fama

Corollario 3.21 (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. Chiaramente $\mathrm{ht}(\mathfrak{p}) \leq 1$, perché l'ideale $(x)^e$ è $\mathfrak{p}^e$-primario in $A_\mathfrak{p}$. Bisogna allora mostrare che $\mathrm{ht}(\mathfrak{p}) \geq 1$. D'altronde, se fosse 0, $\mathfrak{p}$ sarebbe un ideale primo associato a (0). Poiché l'anello è noetheriano, per la decomposizione primaria si ha che 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, dunque $\mathrm{ht}(\mathfrak{p}) = 1$. □

Notiamo che avevamo già dimostrato nella Proposizione 1.52 che, se A è noetheriano, ogni primo $\mathfrak{p}$ propriamente contenuto in un ideale proprio e principale ha altezza 0. Il seguente corollario ha rilevanza in quanto permette di conoscere il comportamento della dimensione rispetto ai quozienti negli anelli locali noetheriani.

Corollario 3.22. 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 proiezioni $\bar{x}_i$ generino in $A/(x)$ un ideale $\mathfrak{m}/(x)$-primario. Allora $(x, x_1, \ldots, x_m)$ generano un ideale $\mathfrak{m}$-primario, e quindi $\dim A \leq \dim A/(x) + 1$. Per la Proposizione 3.12 se x non è un divisore di 0 si ha $\dim(A/(x)) \leq \dim(A) - 1$. □

[3] Non necessariamente locale.

Concludiamo la sezione con un lungo esercizio:

Esercizio 3.23. Sia A un anello locale noetheriano con ideale massimale m e sia q un ideale m-primario. Allora $\dim(A) = \dim(Gr_q(A))$.

Soluzione. Innanzitutto, abbiamo necessità di indagare sulla natura dei primi minimali del graduato.

Definizione 3.24. Sia B un anello graduato e sia I un ideale di B; definiamo

$$I^h = \bigoplus_{n\in\mathbb{N}} I \cap B_i$$

I^h è per definizione un ideale omogeneo ed è il più grande ideale omogeneo contenuto in I.

Lemma 3.25. Sia B un anello graduato e sia I un ideale omogeneo. Supponiamo che per ogni a, b elementi omogenei, valga $ab \in I \Rightarrow a \in I \ \vee \ b \in I$. Allora I è un ideale primo.

Dimostrazione. Consideriamo $x, y \in B$; possiamo scrivere x, y come somma delle loro componenti omogenee

$$x = a_{i_0} + a_{i_1} + \cdots + a_{i_n} \qquad\qquad y = b_{j_0} + b_{j_1} + \cdots + b_{j_m}$$

dove a_{i_k}, b_{j_k} sono omogenei. Possiamo supporre che a_{i_0} e b_{j_0} non stiano in I e che $xy \in I$.

$$xy = a_{i_0}b_{j_0} + \cdots + a_{i_n}b_{j_m}$$

Dato che I è omogeneo, ogni componente del prodotto deve appartenere a I; dato che per gli elementi omogenei $ab \in I$ implica $a \in I$ o $b \in I$, questo deve valere anche per a_{i_0} e b_{j_0}, da cui una contraddizione. □

Lemma 3.26. Sia B un anello graduato e sia I un ideale di B. Se I è un ideale primo, allora I^h è un ideale primo.

Dimostrazione. Siano $x, y \in B$ omogenei tali che $xy \in I^h$; allora in particolare $xy \in I$, da cui $x \in I$ oppure $y \in I$ per primalità di I. Dato che x, y sono omogenei, necessariamente $x \in I^h$ oppure $y \in I^h$, dunque I^h è primo. □

Proposizione 3.27. Sia B un anello graduato e sia P un primo minimale di B. Allora P è omogeneo.

Dimostrazione. Sia P un primo minimale B; allora $P^h \subseteq P$ è un primo di B. Per minimalità di P, $P = P^h$. □

Restringiamoci ora al caso particolare dell'anello graduato.

$$Gr_q(A) = {}^{A}\!/_{q} \oplus {}^{q}\!/_{q^2} \oplus {}^{q^2}\!/_{q^3} \oplus \dots$$

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/q è locale di dimensione 0, il quoziente $Gr_q(A)/I$ è una K-algebra finitamente generata che è anche un dominio; tutti gli ideali massimali hanno allora la stessa altezza per catenarietà. Questo vale per ogni ideale minimale di $Gr_q(A)$, dunque è sufficiente calcolare l'altezza dell'ideale omogeneo

$$P = {}^{m}\!/_{q} \oplus {}^{q}\!/_{q^2} \oplus {}^{q^2}\!/_{q^3} \oplus \dots$$

che contiene tutti i primi minimali, perchè questi ultimi sono omogenei. Per calcolare questo, localizziamo $Gr_q(A)$ rispetto all'ideale P e calcoliamo il graduato rispetto all'ideale

$$Q = (0 \oplus {}^{q}\!/_{q^2} \oplus {}^{q^2}\!/_{q^3} \oplus \dots)^e$$

Otteniamo quindi

$$Gr_{Q^e}((Gr_q(A))_P) = {}^{(Gr_q(A))_P}\!/_{Q^e} \oplus {}^{Q^e}\!/_{(Q^e)^2} \oplus \dots$$

Sorprendentemente,

$${}^{(Gr_q(A))_P}\!/_{Q^e} \simeq {}^{A}\!/_{q}$$

e per ogni termine

$${}^{(Q^e)^n}\!/_{(Q^e)^{n+1}} \simeq {}^{q^n}\!/_{q^{n+1}}$$

da cui l'isomorfismo

$$Gr_{Q^e}((Gr_q(A))_P) \simeq Gr_q(A)$$

Dato che $\dim(A) = d(Gr_q(A))$ e $\dim((Gr_q(A))_P) = d(Gr_{Q^e}((Gr_q(A))_P)) = d(Gr_q(A))$, si ottiene la tesi. □

3.3 Anelli Locali Regolari

Enunciamo precisamente la definizione anticipata

Definizione 3.28. Un anello noetheriano locale di dimensione d si dice *locale regolare* se il suo ideale massimale è generato da d generatori.

Notiamo quindi che per noi un anello locale regolare è anche noetheriano. Per comprendere meglio la definizione, diamo un esempio:

Esempio 3.29. 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 $\dim A = 1$. Dato che A è un dominio, sappiamo che tutti i massimali hanno la stessa altezza e dunque vale $\dim B = \dim C = 1$.
Mostriamo che B è regolare; vogliamo cioè mostrare che l'ideale massimale $(x-1, y-1)^e$ può essere generato con un elemento. Dalla relazione $y^2 - x^3 = 0$ otteniamo

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

Notiamo che $y+1$ è invertibile in B perché $y + 1 \notin (x-1, y-1)$ e dunque

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

per cui B è regolare. C invece non è regolare:

Esercizio 3.30. 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:

1. $\operatorname{gr}_{\mathfrak{m}} A = K[T_1, \dots, T_{\dim A}]$ (implicherà che A è un dominio)
2. $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = \dim A$

Ci serve prima la seguente proposizione:

Proposizione 3.31. Sia A un anello locale noetheriano di dimensione d e sia $\mathfrak{q} = (x_1, \dots, x_d)$ un ideale $\mathfrak{m}$-primario[4]. 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. Consideriamo la mappa di anelli graduati[5]

$$\begin{array}{rccc} \vartheta\colon & {}^{A}\!/_{\mathfrak{q}}[T_1, \dots, T_d] & \longrightarrow & \operatorname{gr}_{\mathfrak{q}}(A) \\ & T_i & \longmapsto & \bar{x}_i \end{array}$$

dove $\bar{x}_i = \pi(x_i)$ e π è il passaggio al quoziente modulo $\mathfrak{q}$. Consideriamo $\bar{f} \in A/\mathfrak{q}[T_1, \dots, T_d]$; per ipotesi, $\bar{f} \in \operatorname{Ker} \vartheta$. Supponiamo per assurdo che qualche coefficiente di f sia invertibile (ossia $\notin \mathfrak{m}$). Allora $\bar{f}$ non è[6] un divisore di 0. Allora

$$d(\operatorname{gr}_{\mathfrak{q}} A) \leq d\left({}^{A/\mathfrak{q}[T_1, \dots, T_d]}\!/_{(\bar{f})}\right) = d(A/\mathfrak{q}[T_1, \dots, T_d]) - 1 = d - 1$$

dove d è l'ordine del polo nella serie di Hilbert-Poincaré. D'altronde, per il Teorema della Dimensione, $d(\operatorname{gr}_{\mathfrak{q}} A) = d$ e questo fornisce un assurdo. □

[4] Spesso, visto che $x_1, \dots, x_d$ realizzano il minimo numero di generatori di un ideale $\mathfrak{m}$-primario, vengono chiamati un *sistema di parametri*.

[5] Si intende che manda omogenei in omogenei. Nel nostro caso rispetta anche il grado, ma non è richiesto.

[6] Per l'Esercizio 3 del Capitolo I dell'Atiyah sappiamo che $g \in B[x]$ è un divisore di 0 se e solo se è annullato da $b \in B$.

Teorema 3.32. Sia A anello locale noetheriano di dimensione d, $\mathfrak{m}$ il suo ideale massimale e $K = A/\mathfrak{m}$. Allora sono equivalenti:

1. $\mathrm{gr}_{\mathfrak{m}} A \cong K[T_1, \ldots, T_d]$
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 e definizione di $\delta(A)$.

$(3 \Rightarrow 1)$ Usiamo la $\vartheta\colon A/\mathfrak{m}[T_1, \ldots, T_d] \to \mathrm{gr}_{\mathfrak{m}} A$ della Proposizione precedente, che sappiamo essere surgettiva. Sappiamo che se $\bar{f} \in \operatorname{Ker}\vartheta$ allora $\bar{f} = 0$, ma allora ϑ è un isomorfismo.

□

Esercizio 3.33. Siano $A = \mathbb{Z}[X, Y, Z]$, $\mathfrak{p} = (7, X, Y, Z)$, e $B = A_{\mathfrak{p}}/(z^2 - x^3 - x - y^2)$. L'anello B è locale regolare?

Soluzione. Per prima cosa 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 può essere vista quozientando, per gli ultimi tre, o via irriducibilità in un UFD per il primo. 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 $\dim B \geq 3$. Inoltre in B vale (tralasciamo i $\bar{}$) $Z^4 - X^3 - X - Y^2 = 0$, e dunque $(ZY)(Z + Y) = X(X^2 + 1)$. Dato che $X^2 + 1$ è invertibile in B possiamo scrivere $\mathfrak{p} = (7, Y, Z)$ e dunque $\dim B \leq 3$ e B è regolare. □

Proposizione 3.34. Sia R 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 $\dim(R[x]) \leq 2d + 1$.

Soluzione. 1. Possiamo supporre $\mathfrak{p}^e = \mathfrak{p}[x] = \mathfrak{q}_1$, 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 $K(R/\mathfrak{p})[X] = S^{-1}R/\mathfrak{p}[x]$. Dato che $\bar{\mathfrak{q}}_2 \cap R/\mathfrak{p} = \emptyset$ e $\bar{\mathfrak{q}}_3 \cap R/\mathfrak{p} = \emptyset$, per la nota corrispondenza fra ideali negli anelli di frazioni abbiamo dunque 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.

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 $d+1$.

□

Lemma 3.35. Se $\bigcap_{j=1}^{\infty} I^j = (0)$ allora $\mathrm{gr}_I(A)$ dominio implica A dominio.

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. □

Proposizione 3.36. Un anello locale regolare è un dominio.

Dimostrazione. Sappiamo già che $\mathrm{gr}_{\mathfrak{m}} A \cong k[T_1, \ldots, T_d]$, e quindi è un dominio. Per il Teorema di Intersezione di Krull $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$. □

Vediamo ora al variare della dimensione di caratterizzare gli anelli locali regolari.
Un anello locale regolare di dimensione 0, dato che deve essere noetheriano per definizione, è artiniano. Per regolarità il suo ideale massimale è generato da 0 elementi, e dunque è (0)[7]. Ne segue che gli anelli locali regolari di dimensione 0 sono i campi.

Se invece A è locale regolare di dimensione 1, allora il suo ideale massimale è principale $\mathfrak{m} = (x)$. In questo caso A è un dominio, e prende il nome di *anello di valutazione discreta*. Questo genere di anelli è trattato sull'Atiyah-Macdonald, ma noi non approfondiremo la questione. A titolo informativo comunque diciamo che

[7] Altermativamente, $\dim \mathfrak{m}/\mathfrak{m}^2 = 0$, cioè $\mathfrak{m} = \mathfrak{m}^2$, e si conclude per Nakayama.

Definizione 3.37. 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*.

I domini di Dedekind sono anche caratterizzati dalla proprietà che ogni ideale si fattorizza unicamente come prodotto di primi.

3.4 Il Teorema della Dimensione della Fibra

Per parlare del Teorema di Dimensione della Fibra abbiamo bisogno di alcuni lemmi preliminari e di un teorema di Going-Down in ipotesi di piattezza:

Lemma 3.38. Siano $f\colon A \to B$ e $g\colon B \to C$ mappe piatte. Allora $g \circ f\colon A \to C$ è piatta.

Dimostrazione. Presa un omomorfismo di A moduli iniettivo $0 \to M \to N$, si ha

$$\begin{gathered} 0 \to N \to M \text{ è iniettiva} \\ \Longleftrightarrow \\ 0 \to B \otimes_A N \to B \otimes_A M \text{ è iniettiva} \\ \Longleftrightarrow \\ 0 \to C \otimes_B B \otimes_A N \to C \otimes_B B \otimes_A M \text{ è iniettiva} \\ \Longleftrightarrow \\ 0 \to C \otimes_A N \to C \otimes_A M \text{ è iniettiva} \end{gathered}$$

da cui la piattezza di C come A-modulo. □

Lemma 3.39. Sia $R \to R'$ piatto e sia S una R-algebra. Allora $S \to S \otimes_R R'$ è piatta.

Dimostrazione. Consideriamo l'omomorfismo iniettivo di S-moduli

$$0 \to N \to M$$

Sicuramente, dato che $M \cong M \otimes_S S$ abbiamo

$$0 \to N \otimes_S S \to M \otimes_S S$$

e guardiamola come successione di R-moduli. Tensorizziamo per R' ottenendo, 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 si conclude con l'associatività del prodotto tensore. □

Teorema 3.40 (Going Down, caso piatto)**.** Sia $f\colon R \to R'$ una mappa piatta di anelli noetheriani, e supponiamo di avere $\mathfrak{q}$ primo di R' e $\mathfrak{p} \supsetneq \mathfrak{p}_0$ primi di R tali che $\mathfrak{q}^c = \mathfrak{p}$. Allora esiste un primo $\mathfrak{q}_0 \subseteq \mathfrak{q}$ di R' tale che $\mathfrak{q}_0^c = \mathfrak{p}_0$.

Dimostrazione. Dato che $R'_\mathfrak{q}$ è piatto, possiamo lavorare in $R'_\mathfrak{q}$, a meno di contrarre il $\mathfrak{q}_0$ in $R'_\mathfrak{q}$ a un $\tilde{\mathfrak{q}}_0$ in R'. 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 $\mathfrak{q}_0 \cap R = 0$. Sia $\mathfrak{q}_0$ un primo minimale di R'; mostriamo che $\mathfrak{q}_0$ soddisfa la tesi. Infatti, se fosse $\mathfrak{q}_0^c = \mathfrak{q}_0 \cap R \neq (0)$, sia $x \in \mathfrak{q}_0^c \setminus \{0\}$ e consideriamo la successione esatta

$$0 \to R \xrightarrow{\cdot x} R$$

dove l'esattezza è data dal fatto che R è un dominio. Per piattezza di R' e ottenendo la mappa iniettiva

$$0 \to R \otimes_R R' \xrightarrow{\cdot x \otimes \mathrm{id}} R \otimes_R R'$$

Inoltre $R \otimes_R R'$ è in maniera ovvia isomorfo ad R' e la mappa diventa $f(x)$ perché $x \otimes 1 = 1 \otimes f(x)$. In sostanza giungiamo a

$$0 \to R' \xrightarrow{\cdot f(x)} R'$$

Ma questo è assurdo perché $\cdot f(x)$ non può essere iniettiva: infatti abbiamo scelto $x \in \mathfrak{q}_0^c \setminus \{0\}$, per cui $f(x) \in \mathfrak{q}_0$ è un divisore di 0 perché dato che il nostro anello è noetheriano e quindi 0 ammette decomposizione primaria, i divisori di 0 sono l'unione dei primi associati a 0 e dunque gli elementi di $\mathfrak{q}_0$ sono tutti divisori di 0. □

Abbiamo ora tutti gli strumenti necessari per parlare del Teorema della Dimensione della Fibra. 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 $E \subseteq R$, i

$$V(E) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq E\}$$

Il Teorema della Fibra fornisce una relazione sulla della dimensione della fibra della mappa $f^\#$ fra questi spazi topologici. Prima di enunciare e dimostrare il teorema, ricordiamo che se M è un A-modulo e I è un ideale di A, $A/I \otimes_A M \simeq M/IM$.

Teorema 3.41 (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

$$\dim R' \leq \dim R + \dim {R'}\big/_{\mathfrak{m}R'}$$

Se inoltre f è *piatta*, cioè se R' è un $f(R)$-modulo piatto, allora vale l'uguaglianza.

Dimostrazione. Esibiamo $\dim R + \dim R'/\mathfrak{m}R' = a+b$ elementi che generano un ideale $\mathfrak{m}'$-primario di R'. Prendiamo $x_1, \dots, x_a$ che generano un ideale $\mathfrak{m}$-primario $I = (x_1, \dots, x_a)$ in $\mathfrak{m}$, che devono esistere per il Teorema della Dimensione. Vediamo che $\dim R'/IR' = \dim R'/\mathfrak{m}R'$: prendiamo la mappa surgettiva $\varphi\colon R'/IR' \to R'/\mathfrak{m}R'$ che proietta al quoziente e notiamo che $\operatorname{Ker}\varphi$ è nilpotente perché $\operatorname{Ker}\varphi \cong \mathfrak{m}R'/IR'$ e siccome siamo in un anello noetheriano esiste n tale che $\mathfrak{m}^n \subseteq I$. Dato che il nucleo è nilpotente la dimensione non cala per corrispondenza con gli ideali del quoziente; infatti il nilradicale è contenuto in ogni primo. Scegliamo dunque $y_1, \dots, y_b \in \mathfrak{m}'/IR'$ tali che $J = (y_1, \dots, y_b)$ sia $\mathfrak{m}'/IR'$-primario. Siano $(s_1, \dots, s_b)$ delle controimmagini dei generatori di J secondo la mappa $R' \to R'/IR'$. Allora l'ideale $K = (f(x_1), \dots, f(x_a), s_1, \dots, s_b)$ è $\mathfrak{m}'$-primario. A tal fine, mostriamo che il radicale è massimale. Sia p un primo che contiene K. Allora p contiene IR' perché $f(x_1), \dots, f(x_a) \in p$; allora per corrispondenza l'immagine di p in R'/IR' è un primo che contiene gli elementi $y_1, \dots, y_b$ e dunque l'immagine di p è $\mathfrak{m}'/IR'$. Ancora per corrispondenza, dunque, $p = \mathfrak{m}'$.

Mostriamo ora l'uguaglianza supponendo che $f\colon R \to R'$ sia piatta. Prendiamo una catena di primi in $R'/\mathfrak{m}R'$

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_b$$

e solleviamola ad R'

$$\mathfrak{m}R' \subsetneq \check{\mathfrak{q}}_0 \subsetneq \check{\mathfrak{q}}_1 \subsetneq \dots \subsetneq \check{\mathfrak{q}}_b$$

Ora $f^{-1}(\check{\mathfrak{q}}_0) = \mathfrak{m}$, perché $\mathfrak{m} \subseteq f^{-1}(\check{\mathfrak{q}}_0)$ ed $\mathfrak{m}$ è massimale. Ora in R abbiamo una catena di a primi

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_a = f^{-1}(\check{\mathfrak{q}_0}) = \mathfrak{m}$$

e per il Teorema del Going Down nel caso piatto si solleva a una catena di primi in R', da cui la tesi. □

Teorema 3.42. Sia R noetheriano di dimensione finita. Allora $\dim R[X] = \dim R + 1$.

Dimostrazione. Chiaramente $\dim R[X] \geq R + 1$ è facile: se

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$$

è una catena di primi in R, è sufficiente considerare le estensioni

$$\mathfrak{p}_0 R[X] \subsetneq \mathfrak{p}_1 R[X] \subsetneq \dots \subsetneq \mathfrak{p}_n R[X] \subsetneq (x, \mathfrak{p}_n)R[X]$$

Gli ideali $\mathfrak{p}_i R[X]$ sono primi perché $R[X]/\mathfrak{p}_i R[X] \cong (R/\mathfrak{p}_i)[X]$, e $(x, \mathfrak{p}_n)R[X]$ è fornisce come quoziente $R/\mathfrak{p}_i$. Le inclusioni rimangono strette.
Occupiamoci ora dell'altra disuguaglianza. Sia

$$\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_m \subsetneq R[X]$$

una catena di primi di $R[x]$ e poniamo $\mathfrak{p} = \mathfrak{q}_m \cap R$. Otteniamo per la proprietà dei sottoinsiemi moltiplicativi l'omomorfismo γ

$$R_{\mathfrak{p}} \xrightarrow{\gamma} R[x]_{\mathfrak{q}_m}$$

che è una mappa locale, cioè $\gamma(\mathfrak{p}^e) \subseteq \mathfrak{q}_m^e$. Per il Teorema della Fibra,

$$\dim R[X]_{\mathfrak{q}_m} \leq \dim R_{\mathfrak{p}} + \dim \underbrace{R[X]_{\mathfrak{q}_m} \big/ \mathfrak{p} R[X]_{\mathfrak{q}_m}}_{B}$$

Dunque, dato che $\dim R_{\mathfrak{p}} \leq \dim R$, è sufficiente mostrare che $\dim B \leq 1$. Questo deriva direttamente dalla Proposizione 3.34; se infatti esistessero $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ ideali primi di B, per corrispondenza avremmo trovato 3 ideali che si contraggono a $\mathfrak{p}$, assurdo.

□

Grazie a questo Teorema è immediato dire che, ad esempio, $\dim \mathbb{Z}[X, Y] = 3$.

Esercizio 3.43. 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 lo 0. Da ciò segue $m + 1 \leq 3$, e quindi $\dim A/I \leq 2$. Dato che quozientiamo per un ideale generato da due elementi ci potremmo aspettare che la dimensione cali ancora di più, ma questo in realtà non succede. Infatti possiamo scrivere

$$I = (X(X + Y + 1), Y(X - Y + 1))$$

e dunque (occhio che I non è primo)

$$I \subsetneq (X - Y + 1) \subsetneq (X, Y - 1) \subsetneq (X, Y - 1, p)$$

che, quozientando, fornisce una catena di primi in A/I di lunghezza 2. □

Capitolo 4

Algebra Omologica

Iniziamo ora a parlare di algebra omologica. L'obiettivo generale è arrivare a parlare di funtori derivati e studiare i funtori Ext^n e Tor^n. Il primo è collegato alle estensioni di moduli e il secondo al prodotto tensore. Introdurremo il concetto di categoria e tratteremo principalemente le categorie dei moduli $\mathscr{M}$ e dei gruppi abeliani Ab.

4.1 Categorie

Definizione 4.1. Una categoria $\mathcal{C}$ è data da

1. Una classe di *oggetti*;
2. Per ogni coppia di oggetti A, B, un insieme di *morfismi*[1] $\mathcal{C}(A, B)$;
3. Per ogni $A, B, C \in \mathcal{C}$ una legge di composizione $\mathcal{C}(A, B) \times \mathcal{C}(B, C) \to \mathcal{C}(A, C)$.

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 $1_A g = g$ e $f 1_A = f$.

Questa è la definizione di categoria *locally small*, il che vuol dire che non permettiamo ai morfismi fra due oggetti di essere una classe propria. Se anche gli oggetti sono un insieme la categoria si dice *piccola*.

Definizione 4.2. Siano $\mathcal{D}$ e $\mathcal{C}$ categorie. Diciamo che $\mathcal{D}$ è una *sottocategoria* di $\mathcal{C}$ se

[1] Non vanno pensati come funzioni, o perlomeno non sempre: possono per esempio essere relazioni d'ordine parziale.

1. Gli oggetti di $\mathcal{D}$ sono una sottoclasse degli oggetti di $\mathcal{C}$;
2. $\mathcal{D}(X,Y) \subseteq \mathcal{C}(X,Y)$;
3. Se $f \in \mathcal{D}(X,Y)$ e $g \in \mathcal{D}(Y,Z)$, allora $g \circ_{\mathcal{D}} f = g \circ_{\mathcal{C}} f$.

Alcuni esempi di categorie sono i seguenti:

- la categoria σ degli insiemi
- le categorie $\mathscr{M}_\Lambda^\ell$ e $\mathscr{M}_\Lambda^r$ dei Λ-moduli rispettivamente sinistri e destri
- la categoria Ab dei gruppi abeliani
- 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 questo elemento.

Le mappe fra categorie si chiamano *funtori*:

Definizione 4.3. 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. $F(1_X) = 1_{F(X)}$

Dato che esiste il funtore identico, uno potrebbe dire che un funtore F è un isomorfismo se esiste un funtore G per il quale la composizione $F \circ G$ sia l'identità. Tuttavia non è il concetto giusto con cui lavorare, perché i funtori che si considerano sono isomorfismi in un senso più generale, che formalizzeremo più tardi. Alcuni esempi sono dati il funtore $\pi_1\colon$ sp. Top. puntati $\to \mathcal{G}$ (la categoria dei gruppi) e il funtore $F_A\colon \mathscr{M}_\Lambda^\ell \to$ Ab che associa $B \mapsto \mathrm{Hom}_\Lambda(A,B)$.

Definizione 4.4. Data una categoria $\mathcal{C}$ si definisce la categoria $\mathcal{C}^{\mathrm{op}}$ che ha gli stessi oggetti ma $\mathcal{C}^{\mathrm{op}}(X,Y) \equiv \mathcal{C}(Y,X)$.
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 $F(f \circ_{\mathcal{C}} g) = F(g) \circ_{\mathcal{D}} F(f)$. Un funtore controvariante è $\bar{F}_B\colon \mathscr{M}_\Lambda^\ell \to$ Ab che associa $C \mapsto \mathrm{Hom}_\Lambda(C,B)$.
Come preannunciato il concetto di isomorfismo di due categorie non è quello classico:

Definizione 4.5. Siano F e G due funtori $\mathcal{C} \to \mathcal{D}$. Una *trasformazione naturale* t tra F e G[2] assegna ad ogni oggetto $X \in \mathcal{C}$ un morfismo $t_X \in \mathcal{D}(F(X), G(X))$ tale che per ogni $f \in \mathcal{C}(X, Y)$

$$\begin{array}{ccc} F(X) & \xrightarrow{t_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[t_Y]{} & G(Y) \end{array}$$

Inoltre se ogni t_X è un isomorfismo si dice che t è un'*equivalenza naturale*.

Per esempio, nel corso di Algebra Lineare, si studiano gli isomorfismi tra uno spazio vettoriale, il suo duale e il suo biduale. Si diceva però che uno spazio e il suo biduale erano canonicamente isomorfi, mentre lo stesso non valeva per il duale. Consideriamo allora la categoria $\mathcal{V}_K$ degli spazi vettoriali su K (i morfismi sono le applicazioni lineari) e definiamo la famiglia di mappe $\{i_V \mid V \in \mathcal{V}_K\}$

$$\begin{array}{rccc} i_V\colon & V & \longmapsto & V^{**} \\ & w & \longmapsto & i_V(w) \end{array}$$

dove $\forall \varphi \in V^*\ i_V(w)(\varphi) = \varphi(w)$. 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 $\varphi^*\colon W^* \to V^*$, $\varphi^*(f) = f \circ \varphi$. Consideriamo ora $**$, il funtore biduale. La i è una trasformazione naturale da Id a $**$, e se ci restringiamo agli spazi di dimensione finita $\mathcal{V}_K^{<+\infty}$ è un'equivalenza naturale.

$$\begin{array}{ccc} \mathrm{Id}(V) & \xrightarrow{i_V} & V^{**} \\ {\scriptstyle \mathrm{Id}(f)}\downarrow & & \downarrow{\scriptstyle f^{**}} \\ \mathrm{Id}(W) & \xrightarrow[i_W]{} & W^{**} \end{array}$$

Il concetto utile sarà quello di *equivalenza di categorie*:

Definizione 4.6. Un'*equivalenza di categorie* è una coppia di funtori le cui composizioni siano naturalmente equivalenti alle rispettive identità.

Esempio 4.7. 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 $\mathcal{B}$,

[2] Una trasformazione naturale non è simmetrica; avere una trasformazione tra F e G non significa averne una tra G e F

$\mathrm{Sym}(X)$ 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?

Dimostrazione. Verifichiamo che le due mappe sono effettivamente funtori.

- Mostriamo la buona definizione 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

$$\begin{aligned}(\mathrm{Sym}(f)) \circ_{\mathcal{S}} (\mathrm{Sym}(g)) &= (\tau \mapsto f\tau f^{-1}) \circ_{\mathcal{S}} (\sigma \mapsto g\sigma g^{-1}) \\ &= (\sigma \mapsto f \underbrace{g\sigma g^{-1}}_{\tau} f^{-1})\end{aligned}$$

- Mostriamo la buona definizione di Ord:
  - $\mathrm{Ord}(\mathrm{id}_X) = \big((x_1, \ldots, x_n) \mapsto (\mathrm{id}_X(x_1), \ldots, \mathrm{id}_X(x_n))\big) = \mathrm{id}_{\mathrm{Ord}(X)}$
  - Da un lato $\mathrm{Ord}(f \circ_{\mathcal{B}} g) = \big((x_1, \ldots, x_n) \mapsto (fg(x_1), \ldots, fg(x_n))\big)$. D'altra parte,

$$\begin{aligned}&(\mathrm{Ord}(f)) \circ_{\mathcal{S}} (\mathrm{Ord}(g))(x_1, \ldots, x_n) \\ &= \big((x_1, \ldots, x_n) \mapsto (f \circ g(x_1), \ldots, f \circ g(x_n))\big)\end{aligned}$$

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

$$\begin{array}{ccc} \mathrm{Sym}(X) & \xrightarrow{\tau_X} & \mathrm{Ord}(X) \\ \Big\downarrow{\scriptstyle \mathrm{Sym}(f)} & & \Big\downarrow{\scriptstyle \mathrm{Ord}(f)} \\ \mathrm{Sym}(X) & \xrightarrow[\tau_X]{} & \mathrm{Ord}(X) \end{array}$$

segue che[3] per ogni $i \in \{1, \ldots, |X|\}$, denotando $(x_1, \ldots, x_n)_i = x_i$,

$$f((\tau_X(\sigma))_i) = (\tau_X(f\sigma f^{-1}))_i$$

[3] Questo semplicemente perché due liste sono uguali se e solo se hanno la stessa lunghezza e lo sono in tutte le posizioni.

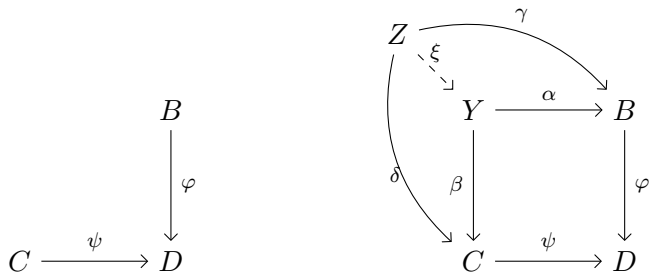
Ora poniamo[4] $f = \sigma$ e sostituendo otteniamo

$$\sigma((\tau_X(\sigma))_i) = (\tau_X(\sigma\sigma\sigma^{-1}))_i = (\tau_X(\sigma))_i$$

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. □

4.1.1 Pullback e Pushout

Definizione 4.8. In una categoria $\mathcal{C}$, dato un diagramma come quello a sinistra, il suo *pullback* è dato da (Y, α, β) tali che esiste sempre unica ξ tale che

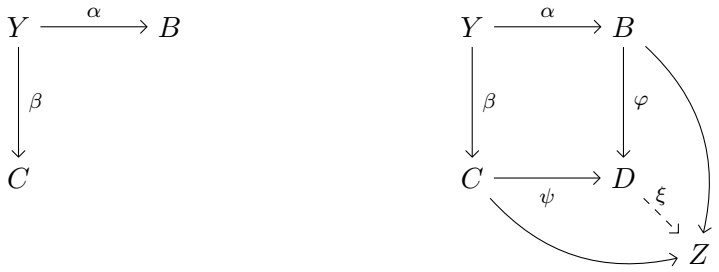


Dalla definizione, se il pullback esiste è unico. Nella categoria $\mathcal{C} = \mathscr{M}_\Lambda$ dei moduli il pullback esiste: si considera la mappa

$$\begin{array}{rccc} \langle\varphi, -\psi\rangle\colon & B \times C & \longrightarrow & D \\ & (b, c) & \longmapsto & \varphi(b) - \psi(c) \end{array}$$

e come $Y = \mathrm{Ker}\langle\varphi, -\psi\rangle$; Y soddisfa la proprietà univerale.

Definizione 4.9. Dato il diagramma a sinistra, il pushout (D, φ, ψ) è il modulo che rende commutativo il diagramma a destra per ogni scelta di Z:



[4]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 oggetti 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 $\sigma \in \mathrm{Sym}(X)$".

Chiaramente, se il pushout esiste, è unico. Nella categoria dei moduli esiste sempre ed è caratterizzato nel modo seguente:

$$D = \frac{B \oplus C}{\mathrm{Im}\langle \alpha, -\beta \rangle} \qquad Y \to B \oplus C \quad y \mapsto (\alpha(y), -\beta(y))$$

Il pushout è una costruzione naturale: per esempio, siano $X = A \cup B$ spazi topologici puntati connessi e localmente connessi per archi, con $A \cup B$ connesso per archi. Abbiamo allora

$$\begin{array}{ccc} A \cap B & \xrightarrow{\subseteq} & A \\ \downarrow{\scriptstyle \subseteq} & & \downarrow \\ B & \longrightarrow & A \cup B = X \end{array}$$

Applicando il funtore π_1, otteniamo il seguente diagramma nella categoria dei gruppi

$$\begin{array}{ccc} \pi_1(A \cup B) & \xrightarrow{i^*} & \pi_1(A) \\ & \downarrow{\scriptstyle j^*} & \\ & \pi_1(B) & \end{array}$$

Il pushout che completa il quadrato è proprio il pushout

$$\frac{\pi_1(A) * \pi_1(B)}{\langle i_*(a) j_*(a)^{-1} \rangle}$$

Il Teorema di Van Kampen può essere allora riformulato in questo modo: il funtore π_1 porta pushout in pushout. Non tutte le categorie hanno pullback o pushout: la categoria dei moduli liberi su un qualsiasi anello non ammette pushout; la categoria dei moduli finitamente generati su un anello non noetheriano non ammette pullback.

4.2 Moduli Proiettivi e Iniettivi

Dopo questa introduzione sulle categorie, passiamo ora a parlare di alcuni oggetti importanti che si utilizzano in algebra omologica. In questa parte, indicheremo con Λ gli anelli, che supporremo essere unitari ma non necessariamente commutativi. Indichiamo invece con Λ^{op} l'anello che ha come insieme di base "lo stesso" di Λ, i cui elementi però saranno denotati come

$$\Lambda^{\mathrm{op}} = \{\lambda^{\mathrm{op}} \mid \lambda \in \Lambda\}$$

e dove le operazioni sono definite come

$$\lambda_1^{\mathrm{op}} + \lambda_2^{\mathrm{op}} = (\lambda_1 + \lambda_2)^{\mathrm{op}} \qquad (\lambda_1\lambda_2)^{\mathrm{op}} = \lambda_2^{\mathrm{op}}\lambda_1^{\mathrm{op}}$$

La moltiplicazione è quindi quella ereditata da Λ a meno di invertire i termini; notiamo che se l'anello è commutativo si ha $\Lambda \simeq \Lambda^{op}$.

Definizione 4.10. Un Λ-*modulo sinistro* M è un modulo con la usuale definizione. Un Λ-*modulo destro* è un Λ^{op}-modulo sinistro. Se diciamo "modulo" intendiamo "modulo sinistro".

Concretamente possiamo pensare alla moltiplicazione per scalare a destra invece che a sinistra. Quando si moltiplica per due elementi dell'anello l'ordine si scambia e dunque l'operazione coincide con quella di Λ^{op}. Enunciamo ora un po' di risultati senza dimostrazione. Al momento considereremo sull'insieme degli omomorfismi di Λ-moduli tra due moduli assegnati la sola struttura di gruppi abeliani.

Proposizione 4.11. Sia $0 \to B' \xrightarrow{\mu} B \xrightarrow{\epsilon} B''$ una successione esatta di Λ-moduli e sia A è un Λ-modulo. Allora la successione

$$0 \to \mathrm{Hom}(A, B') \xrightarrow{\mu_*} \mathrm{Hom}(A, B) \xrightarrow{\epsilon_*} \mathrm{Hom}(A, B'')$$

è esatta, dove $\epsilon_* : \varphi \mapsto \varphi \circ \epsilon$ e $\mu_* \colon \psi \mapsto \psi \circ \mu$.

Proposizione 4.12. 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 $\mu_* \colon \varphi \mapsto \mu \circ \varphi$ e $\epsilon_* \colon \psi \mapsto \epsilon \circ \psi$.

Notiamo che nelle proposizioni abbiamo perso rispettivamente l'esattezza a destra e a sinistra; effettivamente se consideriamo la successione esatta

$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}\big/_{n\mathbb{Z}} \to 0$$

e prendiamo $A = \mathbb{Z}/n\mathbb{Z}$ allora

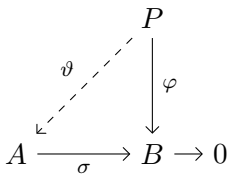
$$0 \to \mathrm{Hom}\left(\mathbb{Z}\big/_{n\mathbb{Z}}, \mathbb{Z}\right) \xrightarrow{(\cdot n)^*} \mathrm{Hom}\left(\mathbb{Z}\big/_{n\mathbb{Z}}, \mathbb{Z}\right) \to \mathrm{Hom}\left(\mathbb{Z}\big/_{n\mathbb{Z}}, \mathbb{Z}\big/_{n\mathbb{Z}}\right)$$

ma l'ultima mappa non è surgettiva. Per mostrare un controesempio per l'altro caso è sufficiente considerare la stessa successione e usare $A = \mathbb{Z}$,

$$0 \to \mathrm{Hom}\left(\mathbb{Z}\big/_{n\mathbb{Z}}, \mathbb{Z}\right) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$$

In questo caso, non c'è la surgettività dell'ultima applicazione, per esempio l'identità $\mathbb{Z} \to \mathbb{Z}$ non appartiene all'immagine (stiamo componendo con la moltiplicazione per n).

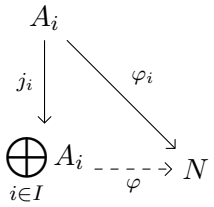
Definizione 4.13. Un modulo P si dice *proiettivo* se esiste ϑ che fa commutare il seguente diagramma[5]



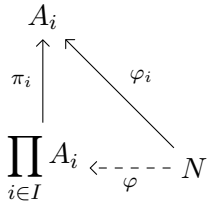
Proposizione 4.14. Ogni modulo libero è proiettivo.

Definizione 4.15. Siano $(A_i)_{i\in I}$ dei 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 $\varphi_i\colon A_i \to N$ esiste un'unico φ che fa commutare i diagrammi



- Il *prodotto diretto* si definisce in maniera analoga ma con tutte le frecce al contrario, dunque i diagrammi sono



Nel caso dei moduli somma e prodotto diretto sono quelli che già conosciamo.

Proposizione 4.16. Sia $A = \bigoplus_{i\in I} A_i$ un Λ-modulo. Allora A è proiettivo se e solo se ogni A_i è un Λ-modulo proiettivo.

Proposizione 4.17. 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 esistono B e ϑ tali che

[5] La "$\to 0$" sta ad indicare che $A \to B$ è surgettiva. La notazione analoga a rovescio verrà usata più avanti per i moduli iniettivi.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i_A} & A \oplus C & \xrightarrow{\pi_C} & C & \longrightarrow & 0 \\ & & \| & & \vdots\,\vartheta & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow[\mu]{} & B & \xrightarrow[\epsilon]{} & C & \longrightarrow & 0 \end{array}$$

e lo stesso risultato vale se esiste $\gamma\colon B \to A$ tale che $\gamma \circ \mu = \mathrm{id}_A$.

Per il Lemma dei Cinque, quando ϑ esiste è un isomorfismo.

Teorema 4.18 (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 4.19. Se Λ è un PID[6] ogni Λ-modulo è proiettivo se e solo se è libero.

In generale questo non è vero. Sia infatti $\Lambda = \mathbb{Z}/12\mathbb{Z}$ e consideriamo l'isomorfismo

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/12\mathbb{Z} \\ ([a], [b]) & \longmapsto & [4a + 3b] \end{array}$$

Λ è un Λ-modulo libero, e quindi proiettivo. Dunque anche $\mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/4\mathbb{Z}$ sono Λ-moduli proiettivi, ma non sono liberi, ad esempio perché hanno torsione.
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 $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
Consideriamo invece la successione esatta di $\mathbb{Z}/p^2\mathbb{Z}$-moduli

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{[1]_p \mapsto [p]_{p^2}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{[m]_{p^2} \mapsto [m]_p} \mathbb{Z}/p\mathbb{Z} \to 0$$

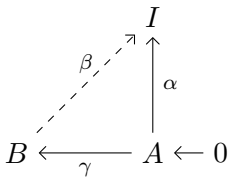
[6] La commutatività è richiesta nella definizione di dominio.

Se $\mathbb{Z}/p\mathbb{Z}$ fosse uno $\mathbb{Z}/p^2\mathbb{Z}$-modulo proiettivo avremmo l'assurdo $\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$; un tale isomorfismo non può esistere neanche come gruppi, perché il secondo non è ciclico.

Esercizio 4.20 (Sfida)**.** Dimostrare che $\prod_{n\in\mathbb{N}} \mathbb{Z}$ non è uno $\mathbb{Z}$-modulo libero (e quindi neppure proiettivo).

Diamo ora la nozione duale di modulo proiettivo:

Definizione 4.21. Un Λ-modulo I si dice *iniettivo* se esiste sempre β che fa commutare



Proposizione 4.22. Un prodotto $\prod_{j\in J} A_j$ è iniettivo se solo se ogni A_j è iniettivo.

Proposizione 4.23. Sia B un Λ-modulo e $\{A_j\}_{j\in J}$ una famiglia di Λ-moduli. Allora

$$\mathrm{Hom}_\Lambda\Big(\bigoplus_{j\in J} A_j, B\Big) \cong \prod_{j\in J} \mathrm{Hom}_\Lambda(A_j, B)$$

dove l'isomorfismo è da intendersi fra gruppi abeliani.

Dimostrazione. È abbastanza ovvio, da un omomorfismo da $\bigoplus$ a B si ricavano tanti omomorfismi $A_j \to B$, e si verifica che la mappa ovvia funziona. □

Per quanto sopra, ponendo $A = B = \mathbb{R}$ si ha che

$$\Big(\bigoplus_{i=0}^{\infty} \mathbb{R}\Big)^* = \prod_{i=0}^{\infty} \mathbb{R}$$

o, in altre parole,

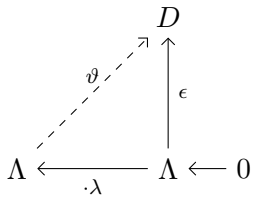
Corollario 4.24. Il duale dei polinomi sono le serie.

Definizione 4.25. Sia Λ un dominio. 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 $\lambda c = d$.

Per esempio, $\mathbb{Q}/\mathbb{Z}$ e $\mathbb{Q}$ sono $\mathbb{Z}$-moduli divisibili, mentre $\mathbb{Z}$ non lo è. Notiamo che in $\mathbb{Q}$, dati $m \in \mathbb{Q}$ e $n \in \mathbb{Z}$, esiste un unico c che soddisfa la definizione. In $\mathbb{Q}/\mathbb{Z}$ questo non è vero: se $d = [0]$ e $\lambda = 4$, come c vanno bene sia $[1/2]$ che $[1/4]$.

Teorema 4.26. Sia Λ un dominio. Allora ogni Λ-modulo iniettivo è divisibile.

Dimostrazione. Siano 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



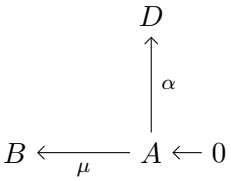
dove $\epsilon(1) = d$ e l'iniettività di $\cdot\lambda$ segue dal fatto che Λ è un dominio. Ora abbiamo

$$\epsilon(1) = \vartheta(\lambda \cdot 1) = \lambda\vartheta(1)$$

e dunque basta porre $c = \vartheta(1)$. □

Teorema 4.27. Sia Λ un PID. Allora ogni Λ-modulo divisibile è iniettivo.

Dimostrazione. Sia D un Λ-modulo divisibile. Vogliamo completare il diagramma



A meno di isomorfismo identifichiamo A con $\mu(A)$ e pensiamo $A \subseteq B$, e consideriamo

$$\Sigma = \{(L, \gamma) \mid A \subseteq L \subseteq B \text{ e } \gamma\colon L \to D, \gamma_{|A} = \alpha\}$$

che è non vuoto perché contiene (A, α). Per Zorn, esiste $(\bar{A}, \bar{\alpha})$ massimale. Supponiamo per assurdo $\bar{A} \neq B$ e sia $b \in B \setminus \bar{A}$. Consideriamo l'ideale di Λ

$$I = \{\lambda \in \Lambda \mid \lambda b \in \bar{A}\} = (\lambda_0) \text{ (perché } \Lambda \text{ è un PID)}$$

Prendiamo poi $\tilde{A} = \langle \bar{A}, b \rangle_\Lambda$ e mostriamo che possiamo estendere $\bar{\alpha}$ ad $\tilde{\alpha}$, contro la massimalità. 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. Definiamo $\tilde{\alpha}\colon \tilde{A} \to D$ come

$$\tilde{\alpha}(\bar{a} + \lambda b) = \bar{\alpha}(\bar{a}) + \lambda c$$

Mostriamo che questa è una buona definizione. Supponiamo $a + \lambda b = a' + \lambda' b$. Allora

$$\underbrace{\bar{a}' - \bar{a}}_{\in \bar{A}} = (\lambda - \lambda')b$$

Quindi $(\lambda - \lambda')b \in \bar{A}$; per definizione di I, $(\lambda - \lambda') \in I$, per cui $\lambda - \lambda' = s\lambda_0$. Ma allora

$$\bar{\alpha}(\bar{a}' - \bar{a}) = \bar{\alpha}(s\lambda_0 b) = s\bar{\alpha}(\lambda_0 b) = s\lambda_0 c = (\lambda - \lambda')c$$

Questo significa che

$$\bar{\alpha}(\bar{a}') + \lambda' c = \bar{\alpha}(\bar{a}) + \lambda c$$

□

Ora vogliamo caratterizzare i moduli iniettivi analogamente a quanto fatto per i proiettivi. Nel farlo vedremo un esempio concreto di una trasformazione naturale fra funtori.

Teorema 4.28. Ogni gruppo abeliano ($\mathbb{Z}$-modulo) può essere immerso in un gruppo abeliano divisibile ($\mathbb{Z}$-modulo iniettivo).

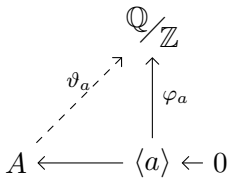
Dimostrazione. Sia A uno $\mathbb{Z}$-modulo e sia $a \in A \setminus \{0\}$. Consideriamo la mappa

$$\langle a \rangle \xrightarrow{\varphi_a} \mathbb{Q}/\mathbb{Z}$$

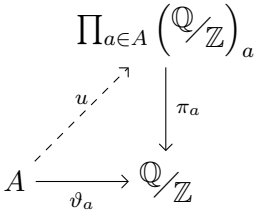
che manda a in

- Un qualunque elemento non nullo se a ha ordine infinito
- Se a ha ordine n, in un elemento di ordine che lo divide.

Per iniettività esiste ϑ_a che fa commutare



Per la proprietà universale del prodotto diretto, esiste u che fa commutare tutti i diagrammi



Ci resta da mostrare che u è iniettiva e in effetti, se $a \neq 0$, guardando la a-esima componente di $u(a)$,

$$\pi_a u(a) = \vartheta_a(a) = \varphi_a(a) \neq 0$$

□

Il modulo $\prod \mathbb{Q}/\mathbb{Z}$ si dice *colibero*, nel senso che vale la proprietà duale a quella dei moduli liberi.

Definizione 4.29. Un Λ-modulo sinistro si dice colibero se è isomorfo a $\prod \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$.

Affinchè questa definizione abbia senso, dobbiamo prima chiarire quale sia la struttura di modulo sul gruppo degli omomorfismi. Siano A un Λ-modulo destro, G uno $\mathbb{Z}$-modulo, e consideriamo $\mathrm{Hom}_{\mathbb{Z}}(A, G)$. Se $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A, G)$ definiamo $\lambda\varphi(a) = \varphi(a\lambda)$. Verifichiamo la buona definizione, cioè che $(\lambda_1\lambda_2)\varphi = \lambda_1(\lambda_2\varphi)$.

$$(\lambda_1\lambda_2)\varphi = \underline{\varphi(a(\lambda_1\lambda_2)) = \varphi((a\lambda_1)\lambda_2)} = \lambda_2\varphi(a\lambda_1) = \lambda_1(\lambda_2\varphi)(a)$$

Notare come la nostra scelta influenzi la parte sottolineata; è importante è che λ_2 agisca per primo.

Teorema 4.30. Siano A un Λ-modulo sinistro, G un gruppo abeliano e consideriamo $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)$ come Λ-modulo sinistro[7]. 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 ogni omomorfismo di Λ-moduli sinistri $\alpha \colon A \to B$ induce il seguente diagramma commutativo:

$$\begin{array}{ccc} \mathrm{Hom}_{\Lambda}(B, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)) & \xrightarrow{\eta_b} & \mathrm{Hom}_{\mathbb{Z}}(B, G) \\ \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \alpha^*} \\ \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G)) & \xrightarrow[\eta_a]{} & \mathrm{Hom}_{\mathbb{Z}}(A, G) \end{array}$$

Risulta quindi definita una equivalenza naturale tra i funtori $\mathrm{Hom}_{\mathbb{Z}}(A, G)$ e $\mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G))$.

Dimostrazione. Definiamo esplicitamente una mappa che associ a 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

$$\eta_A(\varphi)(a) = \varphi(a)(1)$$

Bisogna verificare la buona definizione di questa mappa (esercizio). Per mostrare che è un isomorfismo, forniamo l'inversa $\xi_A = \eta_A^{-1} \colon \mathrm{Hom}_{\mathbb{Z}}(A, G) \to \mathrm{Hom}_{\Lambda}(A, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, G))$ definita come

$$\xi_A(\psi)(a)(\lambda) = \psi(\lambda a) \qquad a \in A,\ \lambda \in \Lambda$$

□

[7] Serve guardare Λ come Λ-modulo destro.

Grazie a questa equivalenza naturale, possiamo ora dimostrare il seguente:

Teorema 4.31. Ogni Λ-modulo sinistro A può essere immerso in un Λ-modulo colibero.

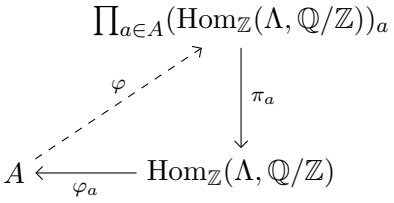
Dimostrazione. A è anche un gruppo abeliano, per cui come già visto nella dimostrazione del Teorema 4.28 per ogni $a \in A$ diverso da 0 esiste una mappa $\vartheta(a)\colon A \to \mathbb{Q}/\mathbb{Z}$ tale che $\vartheta_a(a) \neq 0$. Poniamo

$$\varphi_a = \eta_A^{-1}(\vartheta_a)\colon A \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$$

Per la scelta effettuata,

$$\varphi(a)(1) = \eta_A^{-1}(\vartheta_a)(a)(1) = \vartheta_a(1 \cdot a) = \vartheta_a(a) \neq 0$$

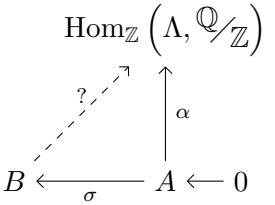
e dunque $\varphi_a(a) \neq 0$. Per la proprietà universale del prodotto diretto, esiste φ che fa commutare i diagrammi



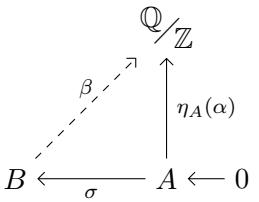
Mostriamo che φ è iniettiva. Sia $a \in A \setminus \{0\}$; allora $\varphi_a(a) \neq 0$ e per commutatività del diagramma $\varphi_a(a) = \pi_a \circ \varphi$ e quindi $\varphi(a) \neq 0$. In particolare $a \notin \mathrm{Ker}(\varphi)$ da cui l'iniettività. □

Teorema 4.32. Ogni Λ-modulo colibero è iniettivo.

Dimostrazione. Dato che il prodotto di moduli iniettivi è iniettivo, basta dimostrare l'iniettività del modulo $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q}/\mathbb{Z})$.



Applichiamo la trasformazione naturale η_A del Teorema 4.30; dato che $\mathbb{Q}/\mathbb{Z}$ è iniettivo, esiste la mappa β



Basta allora considerare la mappa $\eta_B^{-1}(\beta)$ per ottenere la tesi, utilizzando nuovamente il Teorema 4.30. □

Corollario 4.33. Ogni Λ-modulo è sottomodulo di un modulo iniettivo.

Teorema 4.34. Sono equivalenti:

1. I è iniettivo.
2. Il funtore $\mathrm{Hom}(-, I)$ è esatto.
3. Se $0 \to I \to B$ allora esiste un'inversa sinistra.
4. I è addendo diretto di ogni modulo che lo contiene.
5. I è addendo diretto di un modulo colibero.

La dimostrazione si fa con quanto visto finora.

4.3 Funtori Derivati

L'obiettivo è ora quello di definire un funtore derivato. Informalmente, vogliamo lavorare con *complessi*

$$\cdots \to P_4 \to P_3 \to P_2 \to P_1 \to P_0 \to 0$$

dove l'immagine di ogni mappa è inclusa nel nucleo di quella dopo. Supponiamo che successione sia esatta; tramite un funtore T, troviamo un altro complesso

$$\cdots \to TP_4 \to TP_3 \to TP_2 \to TP_1 \to TP_0 \to 0$$

che non è più detto che sia esatto. Possiamo allora studiarne l'omologia, ponendo $H_i = \operatorname{Ker} \delta_i / \operatorname{Im} \delta_{i+1}$. Consideriamo ora un complesso del tipo:

$$P_4 \to P_3 \to P_2 \to P_1 \to P_0 \to A \to 0$$

Applicando T, otteniamo un nuovo funtore che associa ad A i gruppi H_i. Questi si chiamano *funtori derivati* associati a T. Questa è però solo una idea intuitiva; formalizziamo ora la costruzione in maniera rigorosa.

Siano Λ un anello, che consideriamo graduato banalmente (ogni elemento ha grado 0) e $A = \oplus_{\mathbb{Z}} A_i$ un Λ-modulo graduato. Sia $\mathscr{M}_\Lambda^{\mathbb{Z}}$ la categoria dei Λ-moduli graduati, dove un *morfismo di grado* k è un oggetto del tipo $\varphi = \{\varphi_i\}$ dove $\varphi_i \colon A_i \to B_{i+k}$.

Definizione 4.35. 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 $\delta \circ \delta = 0$.

$$\ldots \to C_n \xrightarrow{\delta_n} C_{n-1} \xrightarrow{\delta_{n-1}} C_{n-2} \xrightarrow{\delta_{n-2}} \ldots \to C_1 \to 0$$

Un *morfismo* fra complessi è una $\psi \in \mathscr{M}_\Lambda^{\mathbb{Z}}(C, D)$ di grado 0 che fa commutare

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_n & \xrightarrow{\delta_n} & C_{n-1} & \xrightarrow{\delta_{n-1}} & C_{n-2} & \xrightarrow{\delta_{n-2}} & \cdots \\
 & & \downarrow{\scriptstyle \psi_n} & & \downarrow{\scriptstyle \psi_{n-1}} & & \downarrow{\scriptstyle \psi_{n-2}} & & \\
\cdots & \longrightarrow & D_n & \xrightarrow[\delta'_n]{} & D_{n-1} & \xrightarrow[\delta'_{n-1}]{} & D_{n-2} & \xrightarrow[\delta'_{n-1}]{} & \cdots
\end{array}$$

Risulta quandi definita la categoria Comp_Λ dei complessi.

Definizione 4.36. Una categoria $\mathcal{U}$ si dice *additiva* se

1. Ha l'oggetto 0, cioè un oggetto tale che per ogni altro oggetto A $|\mathcal{U}(0, A)| = |\mathcal{U}(A, 0)| = 1$. In particolare per ogni A, B si può definire un morfismo $0_{A,B}$ come

$$\begin{array}{ccccc}
 & & 0 & & \\
 & \nearrow & & \searrow & \\
A & & \xrightarrow[0_{A,B}]{} & & B
\end{array}$$

2. Ogni coppia di oggetti ha un prodotto

3. Per ogni $A, B \in \mathcal{U}$, $\mathcal{U}(A, B)$ è un gruppo abeliano.

4. La composizione $\mathcal{U}(A, B) \times \mathcal{U}(B, C) \to \mathcal{U}(A, C)$ è bilineare.

Un funtore $T\colon U_1 \to U_2$ categorie additive è *additivo* se per ogni A, B

$$U_1(A, B) \xrightarrow{T} U_2(TA, TB)$$

è un omomorfismo di gruppi abeliani.

Per esempio, le categorie $\mathscr{M}^\ell_\Lambda$, $\mathscr{M}^r_\Lambda$, Comp_Λ sono additive; i funtori fino ad ora introdotti $\mathrm{Hom}(A, -)$, $\mathrm{Hom}(-, A)$, $A \otimes -$, $- \otimes A$ sono additivi.
Notiamo anche che se $T\colon \mathscr{M}^\ell_\Lambda \to \mathscr{M}^\ell_{\Lambda'}$ è additivo e C in Comp_Λ, allora $TC \in \mathrm{Comp}_{\Lambda'}$. In altre parole un funtore additivo manda complessi in complessi[8], per cui T può essere considerato anche come un funtore $T\colon \mathrm{Comp}_\Lambda \to \mathrm{Comp}_{\Lambda'}$.

Definizione 4.37. Sia $C \in \mathrm{Comp}_\Lambda$ un complesso. Definiamo $H_*(C) = \{H_n(C)\}$ come il Λ-modulo graduato tale che $H_n(C) = \operatorname{Ker} \delta_n / \operatorname{Im} \delta_{n+1}$. Chiamiamo quest'ultimo *n-esimo gruppo di omologia*.

[8] Bisogna preservare $\delta \circ \delta = 0$; l'additività implica che l'omomorfismo nullo vada nell'omomorfismo nullo.

Alloo stesso modo si può definire la *coomologia*. Bisogna considerare un complesso del tipo

$$\dots \to C_n \xrightarrow{\delta_n} C_{n-1} \xrightarrow{\delta_{n-1}} C_{n-2} \xrightarrow{\delta_{n-2}} \dots \to C_1 \to 0$$

e si definisce l'*n-esimo gruppo di omologia* come $H^n = \operatorname{Ker}\delta_n / \operatorname{Im}\delta_{n-1}$ e $H_*(C) = \{H^n(C)\}$.

Teorema 4.38. Siano $A, B, C \in \mathrm{Comp}_\Lambda$. Consideriamo il diagramma

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_n & \xrightarrow{\varphi_n} & B_n & \xrightarrow{\psi_n} & C_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta_n} & & \downarrow{\scriptstyle \delta'_n} & & \downarrow{\scriptstyle \delta''_n} & & \\
0 & \longrightarrow & A_{n-1} & \xrightarrow{\varphi_{n-1}} & B_{n-1} & \xrightarrow{\psi_{n-1}} & C_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Allora esiste un omomorfismo ω di moduli graduati di grado -1 che rende esatta la successione

$$\dots \xrightarrow{\omega_{n+1}} H_n(A) \xrightarrow{\varphi_*} H_n(B) \xrightarrow{\psi_*} H_n(C) \xrightarrow{\omega_n} H_{n-1}(A) \to \dots$$

Dimostrazione. Diagram chasing: ω è come nel Lemma del Serpente. □

Siano C e D due complessi di catene e $\varphi, \psi \colon C \to D$ due morfismi di complessi. Queste inducono delle mappe sui moduli di omologia

$$H_*(C) \xrightarrow{\varphi_*} H_*(D) \qquad\qquad H_*(C) \xrightarrow{\psi_*} H_*(D)$$

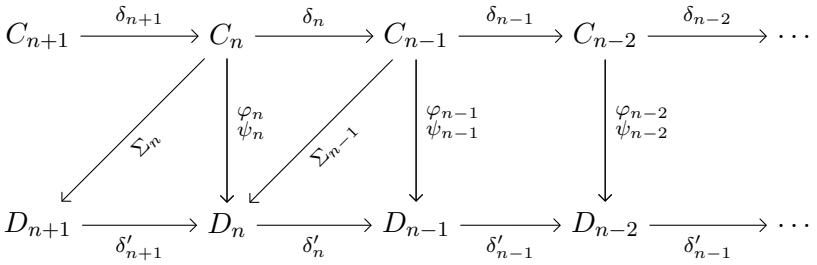
Possiamo capire se $\varphi_* = \psi_*$? Questo è vero se fra loro esiste un'omotopia:

Definizione 4.39. Siano C, D complessi di catene e siano φ, ψ morfismi. 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,

$$\psi - \varphi = \delta' \circ \Sigma + \Sigma \circ \delta$$

ossia per ogni n vale

$$\psi_n - \varphi_n = \delta'_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \delta_n$$



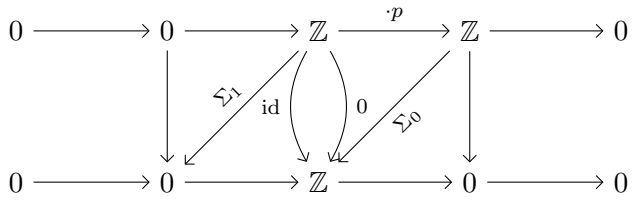
Proposizione 4.40. Se φ e ψ sono omotope allora $\varphi_* = \psi_*$.

Dimostrazione. Bisogna vedere che se $[z] \in H_n(C)$, con $z \in \operatorname{Ker} \delta_n$, allora in $[(\psi_n - \varphi_n)(z)] = [0] \in H_n(D)$. Abbiamo

$$(\psi_n - \varphi_n)(z) = \delta'_{n+1} \circ \Sigma_n(z) + \underbrace{\Sigma_{n-1} \circ \delta_n(z)}_{=0}$$

e dunque $(\psi_n - \varphi_n)(z) \in \operatorname{Im} \delta'_{n+1}$. □

La proposizione viene spesso utilizzata per mostrare che un complesso ha omologia nulla: basta infatti mostrare che l'identità è omotopa a 0. La condizione data nella proposizione è sufficiente ma non necessaria: ci sono morfismi non omotopi che inducono la stessa mappa in omologia.
Consideriamo (C è il complesso di sopra e D quello di sotto, $\varphi \mapsto \varphi_1 = \mathrm{id}$ e $\psi \mapsto \psi_1 = 0$)



Qui $H_0(C) = 0$, $H_1(C) = \mathbb{Z}/p\mathbb{Z}$, $H_0(D) = 0$ e $H_1(D) = \mathbb{Z}$. Le mappe indotte sugli H_1 sono entrambe nulle, una perché indotta dalla mappa nulla e l'altra perché è una mappa da $\mathbb{Z}/p\mathbb{Z}$ a $\mathbb{Z}$, dunque $\varphi_{1*} = \psi_{1*}$ e $\varphi_* = \psi_*$; 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 4.41. Sia $F\colon \mathscr{M}_\Lambda \to \mathscr{M}_{\Lambda'}$ un funtore additivo, $C, D \in \mathrm{Comp}_\Lambda$ e siano φ e ψ omotope. Allora $F(\varphi)$ è omotopa a $F(\psi)$ e l'omotopia è $F(\Sigma)$.

Dimostrazione. Da $\psi - \varphi = \delta' \circ \Sigma + \Sigma \circ \delta$ abbiamo

$$F(\psi) - F(\varphi) = F(\psi - \varphi) = F(\delta') \circ F(\Sigma) + F(\Sigma) \circ F(\delta)$$

dove la prima uguaglianza vale per additività del funtore F. □

Definizione 4.42. 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.

Ne segue che $H(C) \cong H(D)$, e anzi φ_* e ϑ_* sono isomorfismi.

Definizione 4.43. Sia A un Λ-modulo. Una *risoluzione proiettiva* di A è un complesso P tale che

1. Ogni P_j è proiettivo
2. $\operatorname{Coker}\vartheta = H_0(P) \cong A$
3. Per ogni $n \geq 1$ vale $H_n(P) = 0$ (diciamo che P è *aciclico*)

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \begin{array}{c} \longrightarrow \\ \searrow \quad \nearrow \\ A \end{array} 0$$

La prima domanda che sorge spontanea è sotto quali condizioni, dato $A \in \mathscr{M}_\Lambda^\ell$, questo ammetta una risoluzione proiettiva. In realtà, questa esiste sempre, addirittura formata da moduli liberi. Infatti, 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. C'è anche il concetto duale di risoluzione iniettiva, la costruzione è analoga a quella della risoluzione proiettiva usando i Coker invece dei Ker (e passando da moduli coliberi, dato che abbiamo mostrato che ogni modulo si inietta in un modulo colibero).

Definizione 4.44. Siano $T\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ un funtore additivo (covariante), $A \in \mathscr{M}_\Lambda^\ell$ e consideriamo una sua risoluzione proiettiva aciclica

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \begin{array}{c} \longrightarrow \\ \searrow \quad \nearrow \\ A \end{array} 0$$

Definiamo $L_nT(A) \coloneqq H_n(TP)$.

$$TP_n \to TP_{n-1} \longrightarrow \cdots \longrightarrow TP_1 \longrightarrow TP_0 \longrightarrow 0$$

Mostreremo che L_nT è un funtore.
Se T fosse controvariante bisognerebbe considerare

$$0 \to TP_0 \to TP_1 \to TP_2 \to TP_3 \to \cdots$$

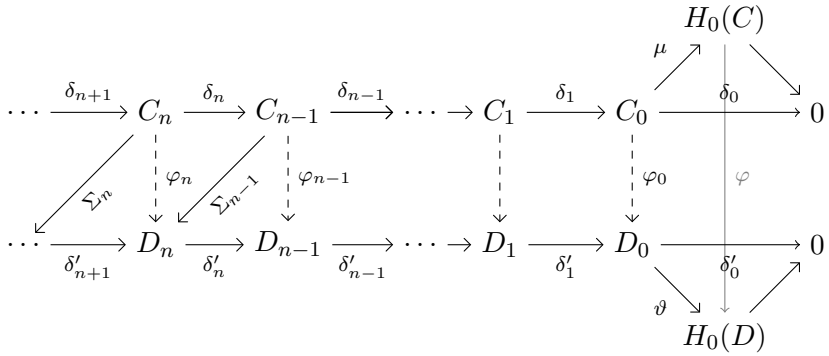
e si pone $R^nT(A) \coloneqq H^n(TP)$ (dove H^n indica la coomologia, mentre l'omologia era H_n).

Analogamente, possiamo ripetere la costruzione con una risoluzione iniettiva. Ad esempio, se T è covariante, dato A, prendiamo una risoluzione iniettiva di A

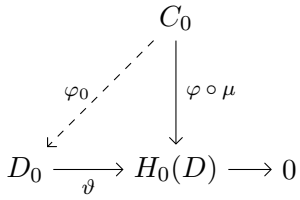
$$\begin{array}{ccccccccccc} 0 & \longrightarrow & I_0 & \longrightarrow & I_1 & \longrightarrow & I_2 & \longrightarrow & I_3 & \longrightarrow & \cdots \\ & \searrow & \nearrow & & & & & & & & \\ & & A & & & & & & & & \end{array}$$

e si pone $R^nT(A) = H^n(TI)$.

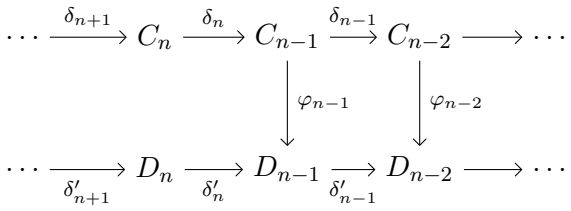
Teorema 4.45. Sia C un complesso positivo[9] aciclico proiettivo e D un complesso positivo e aciclico. Data $\varphi\colon H_0(C) \to H_0(D)$ esiste una mappa di complessi $\bar{\varphi} = \{\varphi_n\}$ che solleva φ. Due tali mappe sono omotope.



Dimostrazione. Procediamo per induzione. φ_0 esiste per proiettività di C_0.

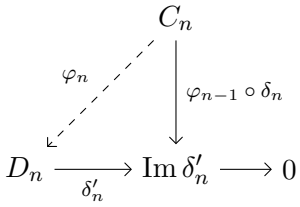


Per il passo induttivo, supponiamo di avere costruito $\varphi_0, \ldots, \varphi_{n-1}$.



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 ne segue $\mathrm{Im}(\varphi_{n-1} \circ \delta_n) \subseteq \mathrm{Ker}\, \delta'_{n-1} = \mathrm{Im}\, \delta'_n$. A questo punto possiamo ottenere φ_n per la proiettività di C_n sul diagramma

[9] Cioè tale che tutti i $C_i = 0$ quando $i < 0$.



Vediamo l'unicità a meno di omotopia. Supponiamo di avere due sollevamenti ψ e ξ. Vogliamo che per ogni n valga

$$\psi_n - \xi_n = \delta'_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \delta_n$$

Poniamo $\Sigma_{-1} = 0$. Per commutatività del diagramma $\operatorname{Im}(\psi_0 - \xi_0) \subseteq \operatorname{Im} \delta'_1 \subseteq \operatorname{Ker} \delta'_0$, dunque Σ_0 esiste per proiettività di C_0 e abbiamo $\psi_0 - \xi_0 = \delta'_1 \circ \Sigma_0$. Per il passo induttivo supponiamo di avere costruito le mappe fino alla Σ_{n-1} e costruiamo la Σ_n. Si può vedere che

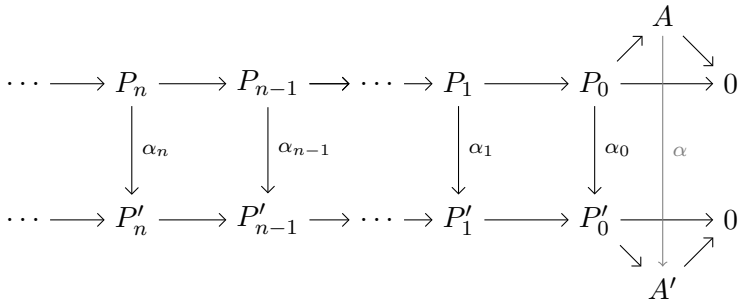
$$\delta'_n(\underbrace{(\psi_n - \xi_n) - \Sigma_{n-1} \circ \delta_n}_{\eta}) = 0$$

e dunque $\operatorname{Im} \eta \subseteq \operatorname{Ker} \delta'_n = \operatorname{Im} \delta'_{n+1}$; di conseguenza Σ_n esiste per proiettività di C_n. Quindi, $\delta'_{n+1} \circ \Sigma_n = \eta$, che scritta per esteso è proprio l'equazione richiesta dall'omotopia. □

Chiaramente, il teorema ammette una versione duale:

Teorema. Siano C, D complessi di cocatene aciclici e positivi e sia D iniettivo. 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.

Torniamo quindi alla situazione iniziale e consideriamo $T\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$ covariante additivo. Siano $A, A' \in \mathscr{M}_\Lambda^\ell$ e prendiamo $\{P_n\}$, $\{P'_n\}$ delle loro risoluzioni proiettive. Vediamo come L_nT agisce sulle mappe. Prendiamo $\alpha\colon A \to A'$. Per il Teorema precedente possiamo sollevare α ad un morfismo di complessi $\bar{\alpha}\colon P \to P'$. Dunque $L_nT(\alpha)$ è $\bar{\alpha}$ passata alle omologie, cioè $L_nT(\alpha) = [T\alpha_n]\colon L_nT(A) \to L_nT(A')$.



Bisogna mostrare che non dipende dalla risoluzione proiettiva scelta. Per farlo si usa il Teorema 4.45 per sollevare l'identità a $\vartheta_n\colon P_n \to Q_n$ e a $\epsilon_n\colon Q_n \to P_n$; dopodiché si invoca sempre lo stesso Teorema per dire che $\bar{\epsilon}\circ\bar{\vartheta}$ è omotopa all'identità, e quindi $T\bar{\epsilon}\circ T\bar{\vartheta} = T(\bar{\mathrm{id}})$. Inoltre questo fornisce un'equivalenza naturale fra $L_n^P T(A)$ e $L_n^Q T(A)$ ottenute con le diverse risoluzioni, che pensiamo come funtori che partono dalla categoria i cui oggetti sono le risoluzioni proiettive di A con morfismi i morfismi che sollevano una certa $\alpha\colon A \to A$. Quella che abbiamo appena esibito è una trasformazione naturale del funtore $L_n^- T$ con sé stesso. Dunque i funtori derivati non solo non dipendono dalla risoluzione proiettiva scelta, ma l'isomorfismo è canonico.

Definizione 4.46. Sia $T = \mathrm{Hom}(-, B)\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$, siano $A \in \mathscr{M}_\Lambda^\ell$ e $\{P_n\}$ una sua risoluzione proiettiva. Definiamo $\mathrm{Ext}^n(A, B)$ il funtore dato da $R^n \mathrm{Hom}(-, B)(A)$.

Dalla definizione, si ottiene che $\mathrm{Ext}^0(A, B) = \mathrm{Hom}(A, B)$. Vedremo che $\mathrm{Ext}^1(A, B)$ misura le successioni esatte

$$0 \to B \to E \to A \to 0$$

Dunque Ext^1 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). Questo spiega anche il perché del nome.

Definizione 4.47. Consideriamo il funtore $A \otimes_\Lambda -\colon \mathscr{M}_\Lambda^\ell \to \mathrm{Ab}$, dove questa volta[10] $A \in \mathscr{M}_\Lambda^r$. Sia $\{P_n\}$ una risoluzione proiettiva di B; poniamo $\mathrm{Tor}_n(A, B) = L_n(A \otimes -)(B) (= H_n(A \otimes B))$.

Data una risoluzione $\{P_n\}$, si applica il funtore $A \otimes -$ e si ottiene che $\mathrm{Tor}_0(A, B) \cong \mathrm{Coker}\,\delta_1 \cong A \otimes B$. Invece Tor^1 "estrae" la parte di torsione, ma vedremo più nel dettaglio. Notiamo che se B è proiettivo una sua risoluzione proiettiva è

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow B \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$B$$

Di conseguenza, applicando il tensore abbiamo

$$\cdots \to A \otimes 0 \to A \otimes 0 \to A \otimes B \to 0$$

e quindi per ogni $j \geq 1$ vale $\mathrm{Tor}_j(A, B) = 0$. Allo stesso modo, se A è un Λ-modulo piatto, si ha lo stesso risultato (il tensore per moduli piatti manda successioni esatte in successioni esatte).
Abbiamo dunque visto che una scelta accurata della risoluzione proiettiva può fare la differenza. In letteratura Ext^1 e Tor_1 vengono costruiti anche con una *presentazione* proiettiva di B.

[10] Perché il prodotto tensore funzioni serve che A sia destro e B sinistro.

Definizione 4.48. Una *presentazione proiettiva* di un Λ-modulo A è una successione esatta corta

$$0 \longrightarrow N \longrightarrow P \longrightarrow A \longrightarrow 0$$

dove P è proiettivo.

Vediamo il collegamento con quest'altra costruzione.

Proposizione 4.49 (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[11]. Sia T un funtore covariante additivo esatto a destra. Allora

$$L_q T(A) \cong \operatorname{Ker} T_\mu$$

Dimostrazione. Prolunghiamo la risoluzione proiettiva; otteniamo così il diagramma

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_{q+1} & \xrightarrow{\delta_{q+1}} & P_q & \xrightarrow{\delta_q} & P_{q-1} & \longrightarrow & \cdots \\ & & & & & \searrow^{\pi_q} \quad \nearrow_{\mu} & & & \\ & & & & & K_q & & & \\ & & & & \nearrow & & \searrow & & \\ & & & & 0 & & 0 & & \end{array}$$

dove $\delta_q = \mu \circ \pi_q$. Usando l'esattezza a destra di T otteniamo il diagramma commutativo

$$\begin{array}{ccccccccc} & & TP_{q+1} & \xrightarrow{T\delta_{q+1}} & TP_q & \xrightarrow{T\pi_q} & TK_q & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle T\delta_q} & & \downarrow{\scriptstyle T_\mu} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & TP_{q-1} & \xrightarrow[\mathrm{id}]{} & TP_{q-1} & & \end{array}$$

Per il Lemma del Serpente, otteniamo la successione esatta

$$TP_{q+1} \xrightarrow{T\delta_{q+1}} \operatorname{Ker} T\delta_q \to \operatorname{Ker} T_\mu \to 0$$

da cui

$$\operatorname{Ker} T_\mu \cong \operatorname{Ker} T\delta_q \big/ \operatorname{Im} T\delta_{q+1} = L_q T(A)$$

□

[11] Ma K_q non necessariamente.

Nel caso di $\mathrm{Tor}^1(A,B)$ dunque, invece della costruzione mediante una risoluzione proiettiva, possiamo considerare una presentazione proiettiva di B

$$0 \to K_1 \xrightarrow{\mu} P_0 \to B \to 0$$

Per il teorema, $\mathrm{Tor}^1(A,B) = L_1(A\otimes -)(B) \cong \mathrm{Ker}(A\otimes K_1 \to A\otimes P_0)$. Questo a volte viene chiamato Tor e misura "quanto non è esatta" a sinistra la successione coi tensori.

Notiamo che abbiamo solo mostrato l'isomorfismo fra gli oggetti; in realtà si potrebbe mostrare Tor e Tor^1 sono naturalmente equivalenti.

4.4 Il Funtore Ext

Iniziamo a studiare il funtore Ext^1; usando la costruzione di Ext^1 con la risoluzione proiettiva e $T = \mathrm{Hom}(-,B)$, ci interessa il primo gruppo di coomologia H^1 del complesso

$$0 \to \mathrm{Hom}(P_0,B) \to \mathrm{Hom}(P_1,B) \to \mathrm{Hom}(P_2,B) \to \dots$$

(e per Ext^n bisogna prendere l'H^n). La Proposizione delle Risoluzioni Proiettive Interrotte ne ha una duale, la cui dimostrazione è analoga:

Teorema. 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 T un funtore controvariante additivo esatto a sinistra. Allora $R^qT(A) \cong \mathrm{Coker}\, T\mu$.

Dunque possiamo costruire $\mathrm{Ext}^1(A,B)$ anche con una presentazione proiettiva di A

$$0 \to R \xrightarrow{\mu} P \to A \to 0$$

dove P è proiettivo; applicando il funtore otteniamo

$$0 \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(P,B) \xrightarrow{T\mu} \mathrm{Hom}(R,B)$$

Per il Teorema precedente, possiamo ricavare $\mathrm{Ext}^1(A,B)$ mediante gli isomorfismi $\mathrm{Ext}^1(A,B) \cong \mathrm{Coker}\, T\mu \cong \mathrm{Hom}(R,B)/\operatorname{Im} T\mu$[12]. I due funtori, Ext^1 e quello costruito così, che definiamo Ext, sono naturalmente equivalenti.

Definizione 4.50. Siano A, B due Λ-moduli sinistri. Un'*estensione di A tramite B* è una successione esatta corta della forma

$$0 \to B \to E \to A \to 0$$

[12] $T\mu$ è stata chiamata fino ad ora μ^*; utilizzeremo entrambe le notazioni

Chiameremo *estensione banale* l'estensione

$$0 \to B \to A \oplus B \to A \to 0$$

Siano A, B Λ-moduli sinistri. Due estensioni si dicono equivalenti se esiste ψ tale che

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 0 & \longrightarrow & B & \longrightarrow & E_2 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

L'estensione banale esiste sempre; notiamo poi che, per il Lemma dei Cinque, se esiste una ψ come nella definizione di equivalenza, allora è un isomorfismo.

Consideriamo il *bifuntore*

$$E\colon (M_\Lambda^\ell)^{\mathrm{opp}} \times M_\Lambda^\ell \to \mathrm{Set}$$

che manda (A, B) nell'insieme delle classi di equivalenza delle estensioni di A, B. Per come l'abbiamo scritto è controvariante nella prima entrata e covariante nella seconda.

Definizione 4.51. Sia Ab la categoria dei gruppi abeliani e sia Set la categoria degli insiemi. Definiamo il funtore dimenticante $D\colon \mathrm{Ab} \to \mathrm{Set}$, che associa a ogni gruppo abeliano il suo supporto.

Il risultato che vale è il seguente:

Proposizione 4.52. $D \circ \mathrm{Ext}^1$ è naturalmente equivalente ad E.

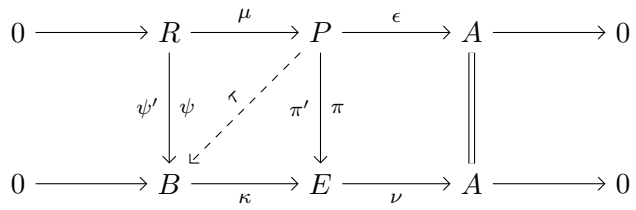
Costruiamo un elemento $\psi \in \mathrm{Hom}(R, B)/\operatorname{Im} T_\mu \cong \mathrm{Ext}^1(A, B)$ a partire da un'estensione

$$0 \to B \to E \to A \to 0$$

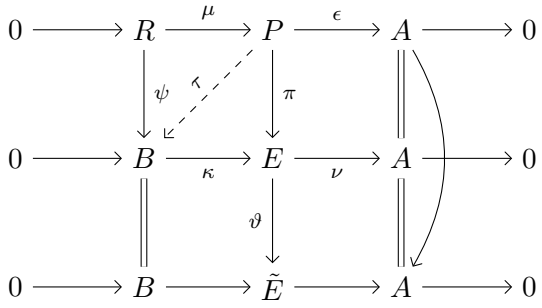
Prendiamo una presentazione proiettiva di A e consideriamo il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & & \vdots{\scriptstyle \psi} & & \downarrow{\scriptstyle \pi} & & \| & & \\ 0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0 \end{array}$$

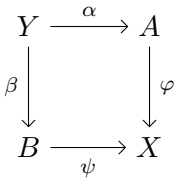
dove π esiste per proiettività di P. Via diagram chasing abbiamo $\operatorname{Im}\pi \circ \mu \subseteq \operatorname{Ker}\nu = \operatorname{Im}\kappa$, per cui possiamo porre $\psi = k^{-1} \circ \pi \circ \mu$. È però necessario necessario mostrare che quanto ottenuto non dipende dalle scelte effettuate. Osserviamo subito che $[\psi]$ non dipende dal sollevamento π, perché se π' è un altro sollevamento abbiamo $\operatorname{Im}(\pi' - \pi) \subset \operatorname{Ker}\nu$, per cui per proiettività di P esiste τ



e abbiamo $\pi' - \pi = \kappa \circ \tau$ e $\psi' - \psi = \tau \circ \mu$. Dunque $[\psi'] = [\psi]$, e anzi questo mostra anche che la costruzione non dipende dalla classe di equivalenza scelta per l'estensione:

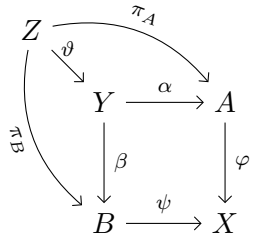


Lemma 4.53. Dato un diagramma di pullback



β induce un isomorfismo fra $\operatorname{Ker}\alpha$ e $\operatorname{Ker}\psi$.

Dimostrazione. Consideriamo il pullback $Z = \operatorname{Ker}\langle\varphi, -\psi\rangle$, 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



Ora ϑ induce un isomorfismo fra $\operatorname{Ker}\pi_A$ e $\operatorname{Ker}\alpha$: infatti

$$\operatorname{Ker}\pi_A = Z \cap \{(0, b) \mid b \in B\} = \{(0, b) \mid b \in \operatorname{Ker}\psi\}$$

perché $(\varphi, -\psi)(0, b) = \varphi(0) - \psi(b) = 0$. Ora $\pi_{B|\operatorname{Ker}\pi_A}$ è sia iniettiva che surgettiva su $\operatorname{Ker}\beta$, quindi è un isomorfismo, e per avere la tesi basta comporre

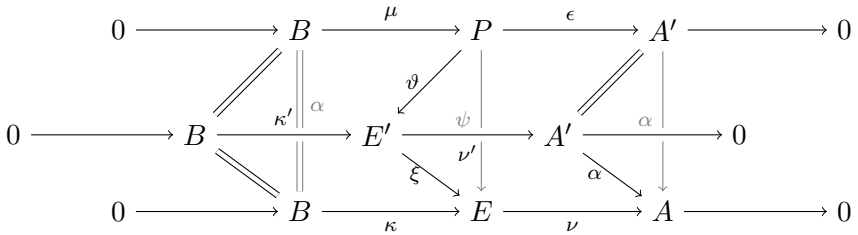
$$\operatorname{Ker}\alpha \xrightarrow{\vartheta^{-1}} \operatorname{Ker}\pi_A \xrightarrow{\pi_B} \operatorname{Ker}\beta$$

□

Lemma 4.54. Se abbiamo un diagramma come sotto, il quadrato a destra è un pullback:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B & \xrightarrow{\kappa'} & E' & \xrightarrow{\nu} & A' & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & B & \xrightarrow[\kappa]{} & E & \xrightarrow[\nu]{} & A & \longrightarrow & 0
\end{array}$$

Dimostrazione. Inseriamo nel diagramma un pullback:



Per il Lemma precedente ψ induce un isomorfismo fra $\operatorname{Ker}\epsilon$ e $\operatorname{Ker}\nu \cong B$. $\operatorname{Ker}\nu = \kappa(B)$. Ora $E' \xrightarrow{\vartheta} P$ per la proprietà di pullback $\psi \circ \vartheta = \xi$ e $\epsilon \circ \vartheta = \nu'$. Vediamo che il quadrato in altro a sinistra commuta. Abbiamo $\epsilon \circ \vartheta \circ \kappa' = \nu' \circ \kappa' = 0$. Allora $\operatorname{Im}\vartheta \circ \kappa' \subseteq \operatorname{Ker}\epsilon$. Abbiamo

$$\psi_{|\operatorname{Ker}\epsilon} \circ \vartheta \circ \kappa' = \xi \circ \kappa' = \kappa = \psi_{|\operatorname{Ker}\epsilon} \circ \nu$$

dunque $\vartheta \circ \kappa' = \nu$ perché $\psi_{|\operatorname{Ker}\epsilon}$ è un isomorfismo. Dunque tutto il diagramma commuta e ϑ è un isomorfismo, dunque il quadrato a destra è un pullback perché isomorfo a un pullback. □

Per il duale del Lemma 4.53 α induce un isomorfismo fra $\operatorname{Coker}\mu$ e $\operatorname{Coker}\beta$, e sappiamo che $\operatorname{Coker}\mu \cong A$, quindi abbiamo verificato che la riga sotto nel diagramma alla fine della sottosezione 4.1.1 è un estensione.

Se ora $[\psi] = [\psi']$ allora $\psi' = \psi + \tau \circ \mu$, otteniamo un diagramma commutativo a batto di aggiungere $\beta\tau$ ad α:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \xrightarrow{\mu} & P & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi} & \overset{\tau}{\swarrow} & \downarrow{\scriptstyle \alpha+\beta\tau} & & \| & & \\
0 & \longrightarrow & B & \xrightarrow[\beta]{} & Y & \xrightarrow[\nu]{} & A & \longrightarrow & 0
\end{array}$$

E quindi per il duale del Lemma precedente il quadrato a destra è un pushout. Dunque la costruzione non dipende da ψ'.

Diamo ora un po' di esempio di calcolo di Ext.
Calcoliamo $\mathrm{Ext}^1(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$. Prendiamo la presentazione proiettiva

$$0 \to \mathbb{Z} \xrightarrow{\cdot 4} \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0$$

e applichiamo Hom

$$0 \to \mathrm{Hom}\left(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\right) \to \mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\right) \xrightarrow{(\cdot 4)^*} \mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\right)$$

Per definizione vale

$$\mathrm{Ext}^1\left(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\right) = \frac{\mathrm{Hom}\left(\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\right)}{\mathrm{Im}(\cdot 4)^*} \cong \frac{\mathbb{Z}/4\mathbb{Z}}{(0)} \cong \mathbb{Z}/4\mathbb{Z}$$

Vediamo chi sono questi quattro elementi. L'estensione banale, che spezza,

$$0 \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0$$

va in 0. Il motivo è che facendo il conto [non riportato, sempre diagram chasing] il sollevamento ψ viene fuori 0. Un altra estensione è

$$0 \to \mathbb{Z}/4\mathbb{Z} \xrightarrow{[a] \mapsto [4a]} \mathbb{Z}/16\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0$$

Vediamo chi è il sollevamento ψ, ma prima dobbiamo sollevare a quella che nel diagramma è φ.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 4} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi(1) = [1]} & & \vdots{\scriptstyle \varphi(n) = [n]_{16}} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \xrightarrow[[a] \mapsto [4a]]{} & \mathbb{Z}/16\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0
\end{array}$$

dunque ψ è l'omomorfismo associato a [1]. Ci mancano gli altri 2. Questa volta invece di partire da un oggetto noto partiamo da ψ e facciamo il pushout. Prendiamo $\psi = 2$, cioè quello che manda 1 in [2].

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 4} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi(1) = [1]} & & \vdots{\scriptstyle \varphi(n) = [n]_{16}} & & & & \\
0 & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \xrightarrow[[a] \mapsto [4a]]{} & \frac{\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}}{\mathrm{Im}\langle \cdot 4, -\psi \rangle} & \longrightarrow & ? & \longrightarrow & 0
\end{array}$$

Chi è "?"? Si vede che $\mathrm{Im}\langle \cdot 4, -\psi\rangle = \langle (4, -[2]_4)\rangle = \langle (4, [2]_4)\rangle$, dunque ci interessa

$$\frac{\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}}{\langle (4, [2]_4)\rangle} = \frac{\mathbb{Z} \oplus \mathbb{Z}}{\langle (0, 4), (4, 2)\rangle}$$

e per capire chi è il signore a destra invochiamo la Forma di Smith: la matrice e le varie mosse sono riportate qui sotto:

$$\begin{pmatrix} 4 & 0 \\ 2 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 4 & -8 \\ 2 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -8 \\ 2 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}$$

e dunque il signore che ci interessava è $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Per $\psi = 3$, anche se non vediamo il conto, l'oggetto nel centro dell'estensione viene sempre $\mathbb{Z}/16\mathbb{Z}$, ma le estensioni *non*sono isomorfe, perché sappiamo l'Ext^1 classifica le estensioni a meno di isomorfismo. La mappa, se prima era la $\cdot 4$, questa volta è la $\cdot 12$. Dunque non ci sono mappe che completano il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \xrightarrow{a \mapsto [4a]} & \mathbb{Z}/16\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 \\ & & \| & & & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \xrightarrow{a \mapsto [16a]} & \mathbb{Z}/16\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 \end{array}$$

e il concetto di estensione è profondamente legato alle mappe e non solo agli oggetti.

Calcoliamo ora $\mathrm{Ext}^1(\mathbb{Z}_{36}, \mathbb{Z}_{42})$ 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

$$\mathrm{Ext}^1(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_m/\langle [n]_m\rangle \cong \mathbb{Z}/\gcd(n, m)$$

E 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 già detto, 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 $(36 \cdot 42 = 1512)$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 36} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{36} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle n \mapsto [n]_{42}} & & \downarrow{\scriptstyle n \mapsto [n]_{1512}} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}_{42} & \xrightarrow[[a] \mapsto [36]]{} & \mathbb{Z}_{1512} & \longrightarrow & \mathbb{Z}_{36} & \longrightarrow & 0
\end{array}$$

e dato che il diagramma commuta, l'estensione è proprio quella.

Il [2] facciamolo per benino, ossia coi pushout:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 36} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{36} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle n \mapsto [2n]_{42}} & & \downarrow{\scriptstyle ?} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}_{42} & \xrightarrow[?]{} & Y & \longrightarrow & \mathbb{Z}_{36} & \longrightarrow & 0
\end{array}$$

Sappiamo che deve essere $Y = (\mathbb{Z} \oplus \mathbb{Z}_{42})/(\mathrm{Im}\langle \cdot 26, -[2n] \rangle)$; ricordiamo che la grafia con $\langle -, - \rangle$ questo 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

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 36} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{36} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle n \mapsto [2n]_{42}} & & \downarrow{\scriptstyle n \mapsto ([0], [n]_{36})} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}_{42} & \xrightarrow[\gamma]{} & \mathbb{Z}_2 \oplus \mathbb{Z}_{756} & \xrightarrow[\delta]{} & \mathbb{Z}_{36} & \longrightarrow & 0
\end{array}$$

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 $\gamma = [a] \mapsto ([n]_2, [36 \cdot 11n]_{756})$, 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 l'esercizio, la corrispondenza è

$$[3] \mapsto \mathbb{Z}_3 \oplus \mathbb{Z}_{504}$$
$$[4] \mapsto \mathbb{Z}_2 \oplus \mathbb{Z}_{756}$$
$$[5] \mapsto \mathbb{Z}_{1512}$$

e anche questa volta le estensioni che danno moduli isomorfi non sono equivalenti. □

Notiamo che, in generale, $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}_m) = 0$ 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 che per ogni $n \geq 1$, $\mathrm{Ext}^n(\mathbb{Z}, A) = 0$. Inoltre abbiamo visto ieri che $\mathrm{Ext}(\mathbb{Z}_m, \mathbb{Z}) \cong \mathbb{Z}_m$ e poco fa che $\mathrm{Ext}(\mathbb{Z}_m, \mathbb{Z}_m) \cong \mathbb{Z}_{\gcd(n,m)}$. Dunque, se A è un gruppo abeliano finitamente generato, per il Teorema di Struttura A è libero se e solo se $\mathrm{Ext}(A, \mathbb{Z}) = 0$, perché $\mathrm{Ext}(\oplus A_i, B) \cong \prod \mathrm{Ext}(A_i, B)$. Che se A è libero $\mathrm{Ext}(A, \mathbb{Z}) = 0$ segue da quanto detto prima. Il viceversa, cioè chiedersi se $\mathrm{Ext}(A, \mathbb{Z}) = 0$ implica A libero, è un questione più delicata. Serre ha mostrato che è vero se A è numerabilmente generato.
Chiaramente quanto fatto fino ad ora con le risoluzioni proiettive può essere fatto anche con le risoluzioni iniettive. 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 $\mathrm{Hom}(A, -)$ e otteniamo

$$0 \to \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, I_1) \to \mathrm{Hom}(A, I_2) \to \dots$$

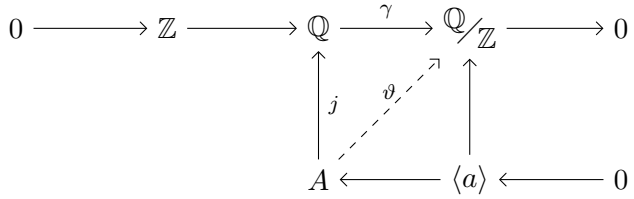
e definiamo $\overline{\mathrm{Ext}}^n(A, -)$ come l'n-esimo funzione derivato destro $R^n(\mathrm{Hom}(A, -))$. Questo è naturalmente equivalente ad Ext^n. Vale cioè che $\overline{\mathrm{Ext}}^n(-, -)$ e $\mathrm{Ext}^n(-, -)$ sono bifuntori naturalmente equivalenti.

Esercizio 4.55. Sia A un gruppo abeliano con torsione. Allora $\overline{\mathrm{Ext}}^1(A, \mathbb{Z}) \neq 0$.

Soluzione. Risolviamo, anzi presentiamo iniettivamente $\mathbb{Z}$:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Sia $a \in A$ un elemento di n-torsione. Per iniettività di $\mathbb{Q}/\mathbb{Z}$ possiamo estendere la mappa $\vartheta(a) = 1/n$ a tutto A



ora j deve per forza essere la mappa nulla ($\mathbb{Q}$ non ha torsione), e quindi ϑ non appartiene all'immagine di γ_*. □

4.5 Funtori Derivati e Successioni Esatte

Il Teorema 4.38 ha la seguente conseguenza sui funtori derivati:

Proposizione 4.56 (Prima successione esatta lunga dei funtori derivati)**.** Sia F un funtore esatto a destra, L_iF i suoi funtori derivati e $0 \to A \to B \to C \to 0$ esatta. Allora è esatta anche

$$\cdots \to L_nFA \to L_nFB \to L_nFC \to L_{n-1}FA \to \cdots$$
$$\cdots \to L_1FC \to FA \to FB \to FC \to 0$$

Dimostrazione. Prendiamo una risoluzione libera di A

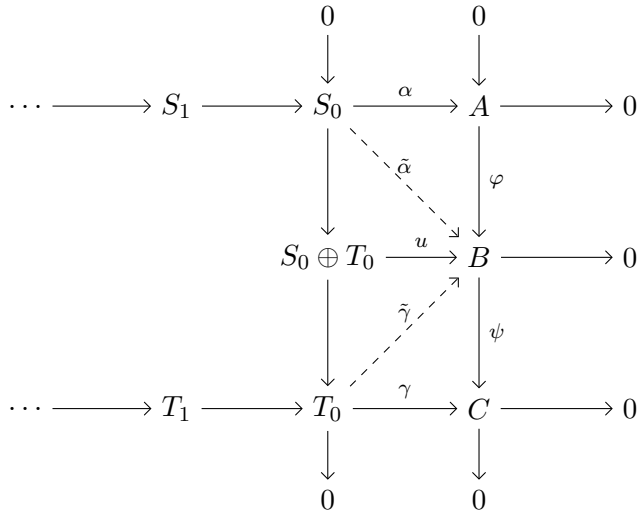
$$\cdots \to S_2 \to S_1 \to S_0 \to A \to 0$$

e una di C

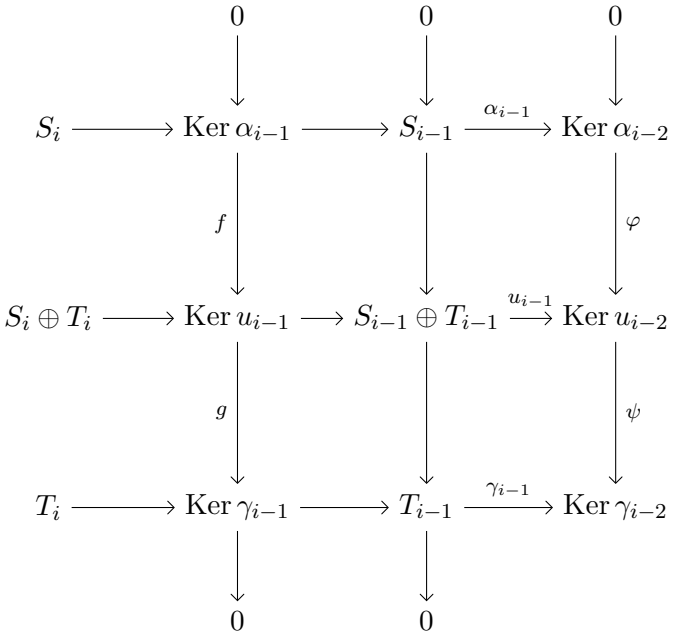
$$\cdots \to T_2 \to T_1 \to T_0 \to C \to 0$$

Mostriamo, per induzione, che possiamo costruirne una per B del tipo

$$\cdots \to S_2 \oplus T_2 \to S_1 \oplus T_1 \to S_0 \oplus T_0 \to B \to 0$$



Mostriamo quindi che esiste $u\colon S_0 \oplus T_0 \to B$ come nel diagramma. Dato che T_0 è libero, è in particolare proiettivo, e dunque esiste $\tilde{\gamma}$ come nel diagramma. Per composizione troviamo $\tilde{\alpha} = \varphi \circ \alpha$. Per la proprietà universale della somma diretta, troviamo allora la $u = \tilde{\alpha} \oplus \tilde{\gamma}$. Tale u fa commutare il diagramma e questo completa il passo base.



Per il passo induttivo, notiamo che per il Lemma del Serpente la mappa g è surgettiva in quanto lo è la mappa α_{i-1} su $\operatorname{Ker}(\alpha_{i-2})$. Ripetendo quanto fatto nel passo base, troviamo allora una mappa $u_i\colon S_i \oplus T_i \to \operatorname{Ker}(u_{i-1})$ surgettiva che quindi rende esatta la successione e fa commutare il diagramma. Induttivamente troviamo così la risoluzione cercata.

Ora applichiamo F e notiamo che per additività del funtore, $F(A \oplus B) \simeq F(A) \oplus F(B)$; la successione del Teorema 4.38 è proprio quella della tesi, dato che $L_0FA = A$, $L_0FB = B$ e $L_0FC = C$. □

La costruzione che abbiamo fatto è naturale, nel senso che se abbiamo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

allora con le successioni esatte lunghe funziona tutto bene. 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.

Teorema 4.57 (Seconda successione esatta lunga per i funtori derivati)**.** Siano F, G, H funtori esatti a destra con due trasformazioni naturali $F \xrightarrow{\varphi} G \xrightarrow{\psi} H$ tali che

- per ogni modulo M valga $\psi_M \circ \varphi_M = 0$
- per ogni modulo proiettivo M la successione

$$0 \to FM \xrightarrow{\varphi_M} GM \xrightarrow{\psi_M} HM \to 0$$

è esatta

Allora esistono dei morfismi $\delta_n \colon L_nHM \to L_{n-1}FM$ che rendono esatta

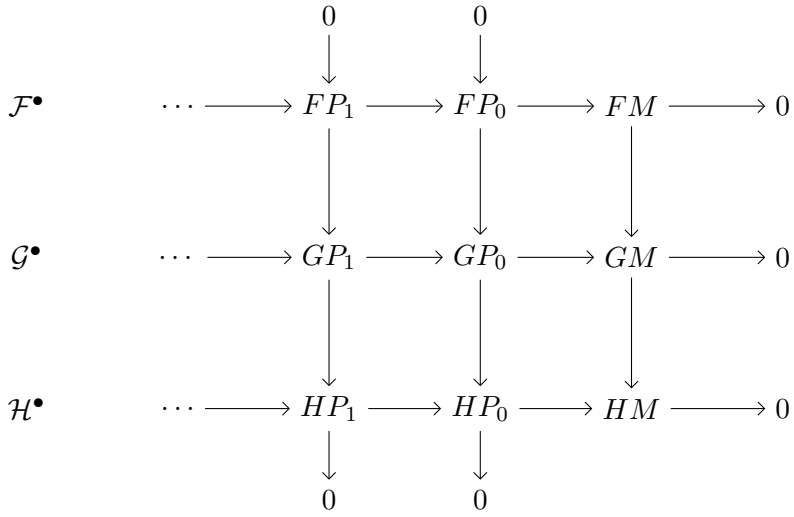
$$\cdots \xrightarrow{L_1\varphi_M} L_1GM \xrightarrow{L_1\psi_M} L_1HM \xrightarrow{\delta_1} FM \xrightarrow{\varphi_M} GM \xrightarrow{\psi_M} HM \to 0$$

e la costruzione è naturale.

Dimostrazione. Prendiamo una risoluzione libera/proiettiva di M

$$P_2 \to P_1 \to P_0 \to M \to 0$$

dai cui otteniamo tre complessi $\mathcal{F}^\bullet$, $\mathcal{G}^\bullet$, $\mathcal{H}^\bullet$ applicandoci i funtori F, G, H.



Le colonne sono esatte per ipotesi. Ricordando che FM, GM e HM per definizione non fanno parte del complesso, si considera la successione esatta lunga in omologia del Teorema 4.38. L'esattezza a destra serve per dire $L_0FA \cong FA$, da cui la tesi. □

4.6 Il Funtore Tor

Dati M, N Λ-moduli, consideriamo i funtori $F \equiv M \otimes_A -\colon \mathscr{M}_A^\ell \to \mathscr{M}_\mathbb{Z}^\ell$ e $G \equiv - \otimes_A N\colon \mathscr{M}_A^r \to \mathscr{M}_\mathbb{Z}^\ell$. Tali funtori sono esatti a destra, e definiamo $\overline{\mathrm{Tor}}_n(M,N) \coloneqq L_nF(N)$ e $\mathrm{Tor}_n(M,N) \coloneqq L_nG(M)$. Come nel caso dell'Ext, questi sono naturalmente equivalenti, ma mostreremo questo in seguito. Mostriamo prima qualche esempio pratico.
Calcoliamo $\mathrm{Tor}_k(\mathbb{Z}_m,\mathbb{Z}_n)$, quindi la costruzione è come funtore derivato di $-\otimes\mathbb{Z}_n$. Prendiamo una risoluzione libera

$$0 \to \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \to \mathbb{Z}_m \to 0$$

e applichiamo il funtore, ottenendo il complesso

$$0 \to \mathbb{Z}\otimes\mathbb{Z}_n \xrightarrow{\cdot m\otimes 1=\mu} \mathbb{Z}\otimes\mathbb{Z}_n \to 0$$

e quindi $L_1F = \mathrm{Tor}_1(\mathbb{Z}_m,\mathbb{Z}_n) = \operatorname{Ker}\mu$ e $L_0F = \mathrm{Tor}_0(\mathbb{Z}_m,\mathbb{Z}_n) = \operatorname{Coker}\mu \cong \mathbb{Z}_m\otimes\mathbb{Z}_n$. I Tor_k per $k>1$ sono tutti nulli perché se estendiamo a sinistra con tutti zeri continuiamo ad avere una risoluzione libera. Il complesso sopra è isomorfo a

$$0 \to \mathbb{Z}_n \xrightarrow{\cdot m=\mu} \mathbb{Z}_n \to 0$$

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

$$\operatorname{Ker} \mu \cong \{x \in \mathbb{Z}_n \mid x \equiv 0 \pmod{n'}\} \cong \mathbb{Z}_d$$

Supponiamo ora A dominio e calcoliamo $\operatorname{Tor}_1(A/(f), M)$, con $f \neq 0$. Prendiamo la risoluzione libera

$$0 \to A \xrightarrow{\cdot f} A \to {}^{A}\!/_{(f)} \to 0$$

(qui stiamo usando A dominio e $f \neq 0$). Come prima consideriamo

$$0 \to A \otimes M \xrightarrow{\cdot f \otimes 1} A \otimes M \to 0$$

e vediamo che $\operatorname{Tor}_k(A/(f), M) = 0$ per $k > 1$, $\operatorname{Tor}_1(A/(f), M) = \{m \in M \mid fm = 0\}$ e $\operatorname{Tor}_0(A/(f), M) = A/(f) \otimes M \cong M/fM$.

Osservazione 4.58.

- Se M è proiettivo, per ogni $n > 0$ $\operatorname{Tor}_n(M, N) = 0$. Basta prendere come risoluzione $0 \to M \to M \to 0$.
- Se $n > 0$ ed N è piatto allora $\operatorname{Tor}_n(M, N) = 0$. Infatti, presa una risoluzione
  $$\ldots \to F_2 \to F_1 \to F_0 \to M \to 0$$
  e applicando $- \otimes_A N$ per piattezza otteniamo una successione esatta e quindi l'omologia è nulla.
- Se usiamo $\overline{\operatorname{Tor}}$ i ruoli di piatto e proiettivo si scambiano.

Vediamo cosa succede alle successioni esatte lunghe dei funtori derivati. Per la prima prendiamo

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

e otteniamo la successione esatta lunga

$$\ldots \operatorname{Tor}_1(M_2, N) \to \operatorname{Tor}_1(M_3, N) \to M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

Per la seconda successione esatta, supponiamo di avere

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

e prendiamo

$$\underbrace{- \otimes N_1}_{F} \xrightarrow{\varphi} \underbrace{- \otimes N_2}_{G} \xrightarrow{\psi} \underbrace{- \otimes N_3}_{H}$$

Dato che proiettivo implica piatto abbiamo anche l'esattezza di

$$0 \to P \otimes N_1 \to P \otimes N_2 \to P \otimes N_3 \to 0$$

e possiamo usare la seconda successione esatta lunga. Questa è

$$\begin{aligned}\ldots \to \operatorname{Tor}_2(M, N_3) \to \operatorname{Tor}_1(M, N_1) \to \operatorname{Tor}_1(M, N_2) \to \\ \to \operatorname{Tor}_1(M, N_3) \to M \otimes N_1 \to M \otimes N_2 \to M \otimes N_3 \to 0\end{aligned}$$

Le stesse osservazioni valgono anche per $\overline{\operatorname{Tor}}$.

Teorema 4.59. $\operatorname{Tor}_k(M, N) \cong \overline{\operatorname{Tor}}_k(M, N)$ e l'isomorfismo è naturale in M ed N.

Dimostrazione. Per induzione su k. Il caso $k = 0$ è ovvio perché entrambi sono $M \otimes N$. Per $k > 0$ prendiamo una presentazione proiettiva di M:

$$0 \to \tilde{M} \to F_0 \to M \to 0$$

Scriviamo la prima successione esatta dei funtori derivati per Tor

$$\underbrace{\operatorname{Tor}_1(F_0, N)}_{=0} \to \operatorname{Tor}_1(M, N) \to \tilde{M} \otimes N \to F_0 \otimes N \to M \otimes N \to 0$$

e se $k \geq 2$

$$0 = \operatorname{Tor}_k(F_0, N) \to \operatorname{Tor}_k(M, N) \xrightarrow{\cong} \operatorname{Tor}_{k-1}(\tilde{M}, N) \to \operatorname{Tor}_{k-1}(F_0, N) = 0$$

Notiamo che stiamo utilizzando il fatto che F_0 sia proiettivo per dire che alcuni gruppi della successione sono 0. Applichiamo la seconda successione esatta per $\overline{\operatorname{Tor}}$ alla presentazione proiettiva di N. Otteniamo la stessa successione ma con $\overline{\operatorname{Tor}}_k$; l'unica differenza è che questa volta per osservare che $\overline{\operatorname{Tor}}_k(F_0, N) = 0$, invece della proiettività bisogna usare la piattezza. Dunque $\overline{Tor}_k(M, N) \cong \overline{Tor}_{k-1}(\tilde{M}, N)$, e basta ragionare per induzione su k partendo dal fatto che per $k = 1$ sono isomorfi perché coincidono col Ker della stessa mappa:

$$0 \to \overline{\operatorname{Tor}}_1(M, N) \to \tilde{M} \otimes N \to F_0 \otimes N \to M \otimes N \to 0$$

□

Proposizione 4.60. Sia R un anello noetheriano locale in $\mathfrak{m}$ e $k = R/\mathfrak{m}$. Sia M un R-modulo finitamente generato. Allora 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 inettiva
5. $\operatorname{Tor}_1(k, M) = 0$

Dimostrazione. Le implicazioni (1) $\Rightarrow$ (2) $\Rightarrow$ (3) sono ovvie.

(3 $\Rightarrow$ 4) La successione $0 \to \mathfrak{m} \to R \to k \to 0$ è esatta. Tensorizzando otteniamo $0 \to \mathfrak{m} \otimes_R M \to R \otimes_R M$ per piattezza di M.

(4 $\Rightarrow$ 5) Consideriamo la successione esatta corta $0 \to \mathfrak{m} \to R \to k \to 0$. Per la prima successione esatta lunga di Tor abbiamo

$$\cdots \to \operatorname{Tor}_1(R, M) \to \operatorname{Tor}_1(k, M) \to \operatorname{Tor}_0(\mathfrak{m}, M) \to \\ \to \operatorname{Tor}_0(R, M) \to \operatorname{Tor}_0(k, M) \to 0$$

Dato che R è libero si ha $\operatorname{Tor}_1(R, M) = 0$. La successione è quindi

$$\cdots \to 0 \to \operatorname{Tor}_1(k, M) \to \underbrace{\mathfrak{m} \otimes_R M \to R \otimes_R M}_{\text{iniettiva per ipotesi}} \to k \otimes_R M \to 0$$

e per esattezza $\operatorname{Tor}_1(k, M) = 0$.

(5 $\Rightarrow$ 1) Siano $x_1, \ldots, x_n$ elementi di M tali che le loro immagini in $M/\mathfrak{m}M$ siano una sua base come k-spazio vettoriale. Per Nakayama $x_1, \ldots, x_n$ generano M come R-modulo. Sia F un R-modulo libero generato da $e_1, \ldots, e_n$. Definiamo $\varphi\colon F \to M$ la mappa definita come $e_i \mapsto x_i$ e sia $E = \operatorname{Ker} \varphi$; otteniamo la successione esatta di R-moduli

$$0 \to E \to F \xrightarrow{\varphi} M \to 0$$

La successione esatta lunga di Tor, pensato come funtore derivato sinistro del funtore $k \otimes_R -$, produce

$$\cdots \to \operatorname{Tor}_1(k, M) \to k \otimes_R E \to k \otimes_R F \xrightarrow{1 \otimes \varphi} k \otimes_R M \to 0$$

Dato che $\operatorname{Tor}_1(k, M) = 0$ per ipotesi, abbiamo

$$0 \to k \otimes_R E \to k \otimes_R F \to k \otimes_R M \to 0$$

Gli oggetti in questione sono diventati ora k-spazi vettoriali; in particolare $k \otimes_R F$ e $k \otimes_R M$ hanno dimensione n, perché $R/\mathfrak{m} \otimes_R M \cong M/\mathfrak{m}M$. Dunque per esattezza $k \otimes_R E = 0$. D'altra parte $k \otimes_R E \cong E/\mathfrak{m}E$, per cui $E = \mathfrak{m}E$. Notiamo che per noetherianità dell'anello, F è un modulo noetheriano e E è isomorfo a un suo sottomodulo. Di conseguenza E è finitamente generato; per Nakayama $E = 0$. Ne segue che $F \cong M$ e M è libero.

□

Lemma 4.61. Sia Λ un PID. Allora ogni Λ-modulo finitamente generato e libero da torsione è libero.

Dimostrazione. Siano M il modulo, $\{y_1, \ldots, y_m\}$ suoi generatori e $\{v_1, \ldots, v_n\}$ un loro sottoinsieme massimale linearmente indipendente. Supponiamo che $y_1 \notin \{v_1, \ldots, v_m\}$. 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 possiamo trovare una tale relazione se $y_1 \in \{v_1, \ldots, v_m\}$. Possiamo ripetere per tutti gli altri y_i, per cui otteniamo delle relazioni

$$\underbrace{a_i}_{\neq 0} y_i + b_{i,1}v_1 + \ldots + b_{i,n}v_n$$

Sia $a = \prod a_i$. Allora

$$0 \to M \xrightarrow{\cdot a} M$$

è iniettiva perché M è libero da torsione. Dunque abbiamo

$$M \cong aM \subset \langle v_1, \ldots, v_n \rangle \cong \Lambda^n$$

Ma allora M è sottomodulo di un modulo libero finitamente generato, e quindi è libero perché Λ è un PID. □

Proposizione 4.62. Sia Λ un PID e sia M è un Λ-modulo. Allora M è piatto se e solo se è libero da torsione.

Dimostrazione.

⇒ Possiamo supporre Λ dominio. Siano $a \in \Lambda$ e $m \in M$ non nulli e tali che $am = 0$. Consideriamo la mappa

$$0 \to \Lambda \xrightarrow{\cdot a} \Lambda$$

che è iniettiva perché Λ è un dominio. Tensorizziamo per M:

$$0 \to \Lambda \otimes M \xrightarrow{\cdot a \otimes \mathrm{id}} \Lambda \otimes M$$

Tale applicazione è iniettiva per piattezza di M. D'altronde,

$$1 \otimes m \xrightarrow{(\cdot a)\otimes \mathrm{id}} a \otimes m = 1 \otimes am = 0$$

dove $1 \otimes m$ è identificato con M nell'isomorfismo $\Lambda \otimes M \cong M$. Ne segue che $m = 0$ e M non ha torsione.

⇐ Sia M libero da torsione e prendiamo una applicazione iniettiva

$$0 \to A' \xrightarrow{\varphi} A$$

Tensorizziamo per M

$$0 \to A' \otimes M \xrightarrow{\varphi\otimes\mathrm{id}} A \otimes M$$

Dobbiamo mostrare che $\varphi \otimes \mathrm{id}$ è iniettiva. Supponiamo per assurdo che non lo sia. Allora esiste un elemento di $A' \otimes M$ che viene mappato a 0

$$\left(\sum a'_i \otimes m_i\right) \xrightarrow{\varphi\otimes\mathrm{id}} 0$$

il che significa che

$$\sum \varphi(a'_i) \otimes m_i = 0 \qquad \text{in } A \otimes M$$

Consideriamo i sotttomoduli $A_0 \subset A$, $A'_0 \subset A'$, $M_0 \subset M$ generati da $\langle a'_i \rangle \subset A'_0$, $\langle \varphi(a'_i) \rangle \subset A_0$ e $\langle m_i \rangle \subset M_0$. Ci riconduciamo quindi alla situazione

$$0 \to A'_0 \to A_0$$

dove però adesso i moduli sono tutti finitamente generati. Ora tensorizziamo per M_0

$$0 \to A'_0 \otimes M_0 \xrightarrow{\varphi\otimes\mathrm{id}} A_0 \otimes M_0$$

e anche stavolta $0 \neq \sum a_i \otimes m_i \mapsto 0$. Dato che Λ è PID, un Λ-modulo finitamente generato e libero da torsione è libero (e in particolare piatto) e abbiamo ottenuto un assurdo.

□

Per esempio, come conseguenza del teorema si ha che $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo piatto.

Esercizio 4.63. Per calcolare $\mathrm{Tor}_k(M, N)$ possiamo utilizzare una risoluzione di M del tipo

$$\ldots F_2 \to F_1 \to F_0 \to M \to 0$$

Mostrare che gli F_i possono essere scelti piatti invece che proiettivi.

Esercizio 4.64. 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 $k \geq 1$.

4.7 Teorema delle Sizigie di Hilbert

Come abbiamo visto in tutta la teoria sui funtori derivati è importante costruire una risoluzione proiettiva/libera di un oggetto dato; sceglierla in maniera accurata può essere talvolta importante.

Definizione 4.65. Se $(A, \mathfrak{m})$ è un anello locale noetheriano, una risoluzione libera di un A-modulo M finitamente generato

$$\ldots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \to 0$$

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. Se $A = \mathbb{K}[t_1, \ldots, t_n]$, con $\mathbb{K}$ campo, e M è finitamente generato e graduato, possiamo prendere una risoluzione di moduli graduati, dove i morfismi δ_i sono morfismi di moduli graduati.

Lemma 4.66. Sia A locale noetheriano e M finitamente generato. Se pensiamo $\mathbb{K} = A/\mathfrak{m}$ come A-modulo, una risoluzione libera

$$\ldots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} M \to 0$$

è minimale se e solo se per ogni $i \geq 1$ la mappa $\bar{\delta}_i \colon F_i \otimes_A \mathbb{K} \to F_{i-1} \otimes \mathbb{K}$ è nulla.

Dimostrazione. Ricordiamo che $N \otimes_A \mathbb{K} = N \otimes_A \mathbb{A}/\mathfrak{m} \cong N/\mathfrak{m}N$, per cui dire che le $\bar{\delta}_i$ sono nulle è equivalente a chiedere che $\operatorname{Im} \delta_i \subseteq \mathfrak{m}F_{i-1}$. Inoltre se N è finitamente generato, il minimo numero di generatori di N è uguale a $b = \dim_{\mathbb{K}} N/\mathfrak{m}N = \dim_{\mathbb{K}} N \otimes \mathbb{K}$ per Nakayama.
Mostriamo l'implicazione "$\Rightarrow$". Tensorizzando la risoluzione troviamo

$$\cdots \to F_1 \otimes \mathbb{K} \xrightarrow{\bar{\delta}_1} F_0 \otimes \mathbb{K} \xrightarrow{\bar{\delta}_0} M/\mathfrak{m}M \to 0$$

Sia $F_0 \otimes \mathbb{K}$ che $M/\mathfrak{m}M$ sono $\mathbb{K}$-spazi vettoriali di dimensione b_0, quindi $\bar{\delta}_1 = 0$.
Per $i > 1$, induttivamente, consideriamo

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & F_i & \xrightarrow{\delta_i} & F_{i-1} & \xrightarrow{\delta_{i-1}} & F_{i-2} & \longrightarrow & 0 \\ & & & & & \searrow \quad \nearrow & & & \\ & & & & & \tilde{M} & & & \\ & & & & 0 & \nearrow \quad \searrow & 0 & & \end{array}$$

Consideriamo la successione

$$\cdots \to F_i \to F_{i-1} \to \tilde{M} \to 0$$

e notiamo che $b_i = \dim_{\mathbb{K}} \tilde{M}/\mathfrak{m}\tilde{M}$. Per lo stesso ragionamento di dimensione, $\bar{\delta}_1 = 0$.

Mostriamo l'altra implicazione "$\Leftarrow$". Qui vale anche per $i = 0$, perché basta notare che da

$$F_1 \otimes \mathbb{K} \xrightarrow{\bar{\delta}_1 = 0} F_0 \otimes \mathbb{K} \xrightarrow{\sim} M \otimes \mathbb{K} \to 0$$

segue che b_0 è il minimo numero di generatori di M. Il caso $i > 0$ segue come prima. □

Definizione 4.67. Sia $(A, \mathfrak{m})$ un anello locale noetheriano e sia M un A-modulo finitamente generato.
La *dimensione proiettiva* $\mathrm{pd}(M)$ di M è il minimo n tale che esiste una sua risoluzione proiettiva lunga n (o $+\infty$ se non ne esistono di lunghezza finita).
La *dimensione globale* di A è

$$\text{gl-dim}(A) = \sup\{\mathrm{pd}(M) \mid M \text{ finitamente generato}\}$$

Chiaramente, se F è un funtore esatto a destra e calcoliamo il funtore derivato $L_iF(M)$, per $i > \mathrm{pd}(M)$ questo è nullo. Vale invece che se A è regolare la dimensione globale coincide con la dimensione come anello. Se A non è regolare è $+\infty$.

Teorema 4.68. Sia $(A, \mathfrak{m})$ un anello locale noetheriano e sia M un A-modulo finitamente generato. Allora coincidono

1. la dimensione proiettiva $\mathrm{pd}(M)$ a
2. la lunghezza di una risoluzione libera minimale di M b
3. $\min\{j \mid \forall i > j \ \mathrm{Tor}_i(A/\mathfrak{m}, M) = 0\}$ c

Inoltre, posto $\mathbb{K} = A/\mathfrak{m}$ e $F_i \cong A^{b_i}$, si ha $b_i = \dim_{\mathbb{K}} \mathrm{Tor}_i(A/\mathfrak{m}, M)$.

Dimostrazione. Chiaramente $b \geq a$ perché ogni risoluzione libera è una risoluzione proiettiva, e $a \geq c$ perché possiamo usare una risoluzione proiettiva che realizza la dimensione proiettiva

$$0 \to F_a \to \ldots \to F_0 \to M \to 0$$

per calcolare Tor. Tensorizzando

$$0 \to \mathbb{K} \otimes F_a \to \ldots \to \mathbb{K} \otimes F_0 \to M \otimes \mathbb{K} \to 0$$

otteniamo subito che i gruppi $\mathrm{Tor}_i(A/\mathfrak{m}, M)$ sono nulli per $i > a$. Inoltre, dato che i $\mathbb{K} \otimes P_i$ sono $\mathbb{K}$-spazi vettoriali, anche i $\mathrm{Tor}_i(\mathbb{K}, M)$ sono $\mathbb{K}$-spazi vettoriali.

Resta da vedere che $c \geq b$. Prendiamo una risoluzione minimale

$$0 \to F_b \to \ldots \to F_i \to F_0 \to m \to 0$$

e vogliamo mostrare che per $0 \leq i \leq b$ vale $\mathrm{Tor}_i(\mathbb{K}, M) \cong \mathbb{K}^{b_i}$. Questo, oltre a $c \geq b$, dimostra anche la seconda parte del Teorema. Per $i = 0$ è vero: $\mathrm{Tor}_0(\mathbb{K}, M) = \mathbb{K} \otimes M$ e per definizione b_0 è la sua dimensione. Per $i > 0$ spezziamo

$$\begin{array}{ccccc} F_i & \longrightarrow & F_{i-1} & \longrightarrow & \cdots \\ & \searrow & \nearrow & & \\ & & \tilde{M} & & \\ & \nearrow & & \searrow & \\ 0 & & & & 0 \end{array}$$

Da una parte $\dim_{\mathbb{K}} \tilde{M} \otimes \mathbb{K} = b_i$. D'altra parte usando $\bar{\delta}_i = 0$ abbiamo che da

$$0 \to F_b \otimes \mathbb{K} \xrightarrow{0} F_{b-1} \otimes \mathbb{K} \xrightarrow{0} \ldots \xrightarrow{0} F_0 \otimes \mathbb{K} \to 0$$

segue che $\mathrm{Tor}_i \simeq F_i \otimes \mathbb{K} = \mathbb{K}^{b_i}$. □

Tutte le osservazioni che abbiamo fatto valgono anche nel caso $A = \mathbb{K}[t_1, \ldots, t_m]$ e considerando solo moduli graduati. Tuttavia per far tornare le cose[13] si "cambia" la definizione di modulo libero dando la possibilità di "cambiare il grado". Ad esempio $M = A^2$ si può graduare come $M_0 = 0$, $M_1 = A_0 \oplus 0$, $M_i = A_{i-1} + A_{i-2}$. In questo contesto per Nakayama M è finitamente generato e graduato $\mathfrak{m}M = M$ implica $M = 0$, che chiaramente vale anche in questo caso graduato. Il tutto può essere enunciato pari pari. Essenzialemente 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 dal quoziente al modulo, ma si rimpiazza con un risultato analogo per i graduati. Ad esempio sia $M = M_0 \oplus M_1 \oplus \ldots$, con $M_0 \neq 0$. Allora $\mathfrak{m}M = M_1 \oplus M_2 \oplus M_3 \ldots$, con $\mathfrak{m} = (t_1, \ldots, t_n)$. Questo è essenzialmente considerato il primo Teorema di algebra omologica. Ci mettiamo nel caso graduato, ma vale anche nel caso locale regolare.

Teorema 4.69 (delle Sizigie di Hilbert)**.** Sia $A = \mathbb{K}[t_1, \ldots, t_n]$ e sia M un A-modulo graduato finitamente generato. Allora M ha una risoluzione libera graduata di lunghezza n.

[13] 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.

Dimostrazione. Vogliamo mostrare che $\mathrm{Tor}_i(\mathbb{K}, M) = 0$ per $i > n$, che per quanto visto è equivalente alla tesi. Per questo ci basta esibire una risoluzione di $\mathbb{K}$ di lunghezza n. Esibiremo la *risoluzione di Koszul*; questa è una risoluzione in A-moduli liberi graduati costruita come segue. Sia $M = A^n \ni t = (t_1, \ldots, t_n)$; indicando con $\bigwedge^i M$ l'i-esimo prodotto esterno definiamo

$$0 \to \bigwedge^0 M \xrightarrow{\partial_n} \bigwedge^1 M \xrightarrow{\partial_{n-1}} \bigwedge^2 M \xrightarrow{\partial_{n-2}} \ldots \to \bigwedge^n M$$

Dove $\partial_i(x) = x \wedge t$. Questo è un complesso perché $t \wedge t = 0$; inoltre F_i è libero ed è isomorfo a $A^{\binom{n}{i}}$, e $\delta_i(F_i) \subset \mathfrak{m}F_{i-1}$. Abbiamo $t = (t_1, \ldots, t_n) = t_1e_1 + \ldots + t_ne_n$, dove $\{e_i\}$ è la base standard di $M = A^n$, e $t \wedge v = \sum t_i(e_i \wedge v)$. Ci basta mostrare che, posto $K_\bullet$ questo complesso,

Lemma 4.70. Se $1 \leq i \leq n$, allora $H_i(K_\bullet) = 0$, mentre $H_0(K_\bullet) \simeq \mathbb{K}$.

Questo conclude perché abbiamo una risoluzione minimale di $\mathbb{K}$ lunga n e quindi $\mathrm{Tor}_i(\mathbb{K}, N) = 0$ per $i > n$.

Dimostrazione del Lemma. Se $r \leq n$ definiamo $M_r = A^r$ e introduciamo un nuov complesso $K^r_\bullet$ definito come

$$0 \to \bigwedge^0 M_r \to \bigwedge^1 M_r \to \ldots \to \bigwedge^r M_r \to 0$$

dove poniamo $x_r = t_1e_1 + \ldots + t_re_r$ e le mappe sono $x_r \wedge -$. Dimostriamo che $H_i(K^r_\bullet) = 0$ per $1 \leq i \leq r$ e $H_0(K^r_\bullet) \cong A/(t_1, \ldots, t_r)$. La tesi del Lemma è il caso $n = r$. Procediamo per induzione su r.
Per $r = 1$ abbiamo $M_1 = A$ e $\bigwedge^0 A \simeq \bigwedge^1 A$, per cui abbiamo

$$0 \to A \xrightarrow{\cdot t_1} A \to 0$$

e la tesi è vera perché la moltiplicazione per t_i è iniettiva. Per il caso induttivo prendiamo

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \bigwedge^0 M_{r+1} & \xrightarrow{x_r \wedge -} & \bigwedge^1 M_{r+1} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow{\scriptstyle - \wedge e_{r+1}} & & \downarrow{\scriptstyle - \wedge e_{r+1}} & & \\
0 & \longrightarrow & \bigwedge^0 M_{r+1} & \xrightarrow{x_{r+1} \wedge -} & \bigwedge^1 M_{r+1} & \xrightarrow{x_{r+1} \wedge -} & \bigwedge^2 M_{r+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \bigwedge^0 \pi} & & \downarrow{\scriptstyle \bigwedge^1 \pi} & & \downarrow & & \\
0 & \longrightarrow & \bigwedge^0 M_r & \longrightarrow & \bigwedge^1 M_r & \longrightarrow & \bigwedge^1 M_r & \longrightarrow & \cdots
\end{array}$$

Abbiamo che $\bigwedge^0 \pi$ è iniettiva è surgettiva, e di fatto è l'identità, e dato che $M_{r+1} = M_r \oplus M_2 \oplus A_{e_{r+1}}$ e $\bigwedge^i M_{r+1} \cong \bigwedge^i M_r \oplus (\bigwedge^{i-1} M_r) \wedge e_{r+1}$ le colonne sono esatte. Via verifiche contose[14] [da aggiungere, me le sono perse] i quadrati commutano tutti. Abbiamo quindi tre complessi e una succesione esatta fra loro, e possiamo scrivere la successione esatta lunga dell'omologia

$$0 \to H_{r+1}(K_{r+1}) \to H_r(K_r) \to H_r(K_r) \to H_{r-1}(K_{r+1}) \to \\ \to H_{r-1}(K_r) \to H_{r-1}(K_r) \to \dots$$

Sappiamo che tutti i termini della successione sono nulli tranne $H_{r+1}(K_{r+1})$ e $H_{r-1}(K_{r+1})$; dunque per esattezza lo sono anche questi due e, almeno per $2 \leq i \leq r+1$, sappiamo che $H_i(K_{r+1}) = 0$. Vediamo cosa succede alla fine della successione. Abbiamo

$$\underbrace{H_2(K_{r+1})}_{=0} \to \underbrace{H_1(K_r)}_{=0} \to \underbrace{H_1(K_r)}_{=0} \to H_1(K_{r+1}) \to \\ \to \underbrace{H_0(K_r)}_{A/(t_1,\dots,t_r)} \to \underbrace{H_0(K_r)}_{A/(t_1,\dots,t_r)} \to H_0(K_{r+1}) \to 0$$

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 (quella del Lemma del Serpente)

$$x_{r+1} \wedge u = f\left(\sum_{i=1}^{r+1} t_i e_i\right) \wedge e_1 \wedge \dots \wedge e_r = f t_{r+1} \wedge e_{r+1} \wedge e_1 \wedge \dots \wedge e_r = \\ = \pm f t_{r+1} \wedge e_1 \wedge \dots \wedge e_{r+1}$$

viene fuori che $\delta(x) = t_{r+1} x$, quindi δ è iniettiva e $H_1(K_{r+1}) = 0$. □

□

Moficiando leggermente la dimostrazione, lo stesso Teorema vale negli anelli locali se $\mathfrak{m} = (t_1, \dots, t_r)$ e $t_i \colon A/(t_1, \dots, t_{i-1}) \to A/(t_1, \dots, t_{i-1})$ è iniettiva. Un tale insieme di generatori si può trovare nel caso in cui A è locale regolare. In questo caso quindi gl-dim$(A) = \dim A$.

Esercizio 4.71. Sia $A = \mathbb{K}[t_1, \dots, t_n]$ e M finitamente generato. Allora M ha una risoluzione proiettiva/libera finita.

4.8 Omologia e Coomologia di Gruppi

Dato un gruppo G costruiamo $\mathbb{Z}[G]$. Questo, come $\mathbb{Z}$-modulo, è il modulo libero su generatori $g \in G$. Dunque un suo elemento è una somma finita

[14] "Il segno viene sbagliato comunque"

$\sum m_g g$, con gli $m_g \in \mathbb{Z}$. Lo muniamo della struttura di anello definendo la moltiplicazione come

$$g \cdot h \mapsto gh$$

Per esempio

$$(3g + 2g') \cdot (6h + 2h^{-1}) = 18gh + 6gh^{-1} + 12g'h + 4g'h^{-1}$$

dove la moltiplicazione gh è la moltiplicazione tra elementi di G. Ad esempio in $\mathbb{Z}[S_3]$

$$\big(2(12) + 3(123)\big)\big(5(13) + 1 \cdot \mathrm{id}\big) = 10(123) + 2(12) + 15(23) + 3(123)$$

e questo è un anello non commutativo.

Ora se G è un gruppo possiamo definire un G-modulo A intendendo che A è un gruppo abeliano e esiste un omomorfismo di gruppi $\Phi\colon G \to \mathrm{Aut}(A)$. Se questo mappa $g \mapsto \varphi_g$, allora

$$g \cdot a = \varphi_g(a) \qquad a \in A$$

Un tale Φ si estende a un omomorfismo di anelli $\tilde{\Phi}\colon \mathbb{Z}[G] \to \mathrm{End}(A)$ (in arrivo non sono più automorfismi perché abbiamo la somma; pensiamo al caso in cui in arrivo c'è un gruppo di matrici...). Questo permette di utilizzare la teoria svolta per i funtori derivati:

Definizione 4.72. Siano G un gruppo e A uno $\mathbb{Z}[G]$-modulo. La *coomologia di G a coefficienti in A* è definita come

$$H^n(G, A) \equiv \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

Notiamo che 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. Lo muniamo della 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

$$(g - h) \cdot n = g \cdot n - h \cdot n = n - n = 0$$

In concreto, per calcolare $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ bisogna prendere una risoluzione proiettiva di $\mathbb{Z}$ come $\mathbb{Z}[G]$-moduli

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$\mathbb{Z}$$

poi applichiamo $\mathrm{Hom}(-, A)$ ottenendo

$$0 \to \mathrm{Hom}(P_0, A) \xrightarrow{\delta_0} \mathrm{Hom}(P_1, A) \xrightarrow{\delta_1} \mathrm{Hom}(P_2, A) \xrightarrow{\delta_2} \dots$$

e calcolandone la coomologia, ad esempio

$$\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, A) = H^2 = \mathrm{Ker}\,\delta_2/\,\mathrm{Im}\,\delta_1$$

Ovviamente è possibile usare equivalentemente una risoluzione iniettiva di A.

Definizione 4.73. Dato G un gruppo e dato uno $\mathbb{Z}[G]$-modulo destro B, l'*omologia di G a coefficienti in B* è

$$H_n(G, B) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(B, \mathbb{Z})$$

Anche qui su $\mathbb{Z}$ si intende messa la struttura di $\mathbb{Z}[G]$-modulo banale.

Lo 0-esimo gruppo di coomologia Indaghiamo sulla struttura del gruppo $H^0(G, A)$; questo è per definizione $\mathrm{Ker}\,\delta_0$. Dato che $\mathrm{Hom}(-, A)$ è esatto a sinistra, possiamo prendere una risoluzione proiettiva e applicare il funtore

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \xrightarrow{\delta_0} \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \xrightarrow{\delta_1} \dots$$

e dunque $H^0(G, A) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.
Notiamo che un elemento φ di $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ è determinato dall'immagine di 1. Inoltre deve soddisfare $\varphi(\lambda x) = \lambda\varphi(x)$. Vogliamo che valga dunque $\varphi(g \cdot 1) = g \cdot \varphi(1)$. 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 parole a è invariante per G, per cui $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G$ è il *sottomodulo degli invarianti*, cioè

$$\{x \in A \mid \forall g \in G\ gx = x\}$$

Quindi il gruppo $H^0(G, A)$ fornisce informazioni sugli invarianti rispetto all'azione di G.

Lo 0-esimo gruppo di omologia Indaghiamo invece sul gruppo di omologia $H_0(G, A)$.

Definizione 4.74. Consideriamo l'omomorfismo di anelli $\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ che manda $\sum m_g g \mapsto \sum m_g$ o, equivalentemente, $\forall g \in G\ \epsilon(g) = 1$. Questo si chiama *augmentazione*. Chiamiamo $IG = \mathrm{Ker}\,\epsilon$ l'*ideale di augmentazione*.

Denotando con e l'identità di G, per ogni $g \in G$ è chiaramente vero che $g - e \in IG$. Ma vale di più:

Proposizione 4.75. *IG è lo $\mathbb{Z}$-modulo libero generato dai $g - e$ al variare di g in $G \setminus \{e\}$.*

Dimostrazione. Chiaramente vale $\langle g-e\rangle_{g\in G,\mathbb{Z}} \subseteq IG$ (lo span è considerato su $\mathbb{Z}$). Viceversa se $\sum m_g g \in \operatorname{Ker}\epsilon$ per definizione vale $\sum m_g = 0$; ma allora basta scrivere

$$\sum m_g g = \sum m_g g - \underbrace{\left(\sum m_g\right)}_{=0} e = \sum m_g(g-e)$$

□

Proposizione 4.76. *IG è generato come $\mathbb{Z}[G]$-modulo dagli $x-e$ al variare di x in un insieme di generatori di G.*

Dimostrazione. Siano x, y geneatori di G. Basta mostrare che $xy-e, x^{-1}-e \in \langle x-e\rangle_{\mathbb{Z}[G]}$ dove x varia nell'insieme di generatori scelto. D'altronde,

- $xy-e = x(y-e)+(x-e)$
- $x^{-1}-e = -x^{-1}(x-e)$

□

Possiamo ora calcolare $H_0(G,B)$; per definizione, questo è il gruppo $\operatorname{Tor}_0^{\mathbb{Z}[G]}(B,\mathbb{Z})$, dove $\mathbb{Z}$ è munito della struttura di $\mathbb{Z}[G]$-modulo banale. Prendiamo 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

$$\ldots \to B \otimes_{\mathbb{Z}[G]} P_2 \to B \otimes_{\mathbb{Z}[G]} P_1 \to B \otimes_{\mathbb{Z}[G]} P_0 \to 0$$

Vista l'esattezza a destra del funtore, abbiamo $B \otimes P_0 \to B \otimes \mathbb{Z} \to 0$. Prendiamo un generatore $b \otimes n$ del prodotto tensore. Abbiamo

$$bg \otimes n = b \otimes gn = b \otimes n$$

Dunque possiamo scrivere

$$B \otimes_{\mathbb{Z}[G]} \mathbb{Z} \cong {}^{B\otimes_{\mathbb{Z}}\mathbb{Z}}\!/_{\langle bg\otimes 1 - b\otimes 1\rangle}$$

Dato che $B \otimes_{\mathbb{Z}} \mathbb{Z} \cong B$ in definitiva abbiamo

$$H_0(G,B) \cong {}^{B}\!/_{\langle bg-b\rangle} = {}^{B}\!/_{\langle b(g-e)\rangle} = {}^{B}\!/_{B\cdot IG}$$

Dalla riga sopra è chiaro che se G agisce su B banalmente allora $H_0(G,B) = B$.

Il primo gruppo di coomologia Studiamo ora il gruppo $H^1(G, A)$.

Definizione 4.77. Sia G un gruppo e A un $\mathbb{Z}[G]$-modulo. Una *derivazione* è una funzione $\varphi\colon G \to A$ tale che

$$\varphi(xy) = \varphi(x) + x\varphi(y)$$

L'insieme delle derivazioni $\mathrm{Der}(G, A)$ è un gruppo abeliano (con la somma).

Segue immediatamente dalla definizione che se φ è una derivazione allora $\varphi(e) = 0$, perché $\varphi(e) = \varphi(e^2) = \varphi(e) + e\varphi(e)$. Dunque $\varphi(e) = 2\varphi(e)$, per cui $\varphi(e) = 0$.

Teorema 4.78. 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. Sia A uno $\mathbb{Z}[G]$-modulo e vediamo chi è $\eta_A\colon \mathrm{Der}(G, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(IG, A)$. Se d è una derivazione diciamo cosa fa $\eta_A(d)$:

$$\eta_A(d)(x - e) = d(x)$$

Questo intanto è un omomorfismo di gruppi abeliani. Verifichiamo che $\eta_A(d)$ è effettivamente un omomorfismo di $\mathbb{Z}[G]$-moduli. Bisogna vedere che

$$\eta_A(d)(g \cdot (x - e)) \stackrel{?}{=} g \cdot \eta_A(d)(x - e)$$

partiamo da sinistra:

$$\begin{aligned}
\eta_A(d)(g(x - e)) &= \eta_A(d)((gx - e) - (g - e)) \\
&= \eta_A(d)(gx - e) - \eta_A(d)(g - e) \\
&= d(gx) - d(g) \\
&= gd(x) \\
&= g \cdot \eta_A(d)(x - e)
\end{aligned}$$

La mappa inversa $\xi_A = \eta_A^{-1}\colon \mathrm{Hom}_{\mathbb{Z}[G]}(IG, A) \to \mathrm{Der}(G, A)$ è definita come

$$\xi_A(\varphi)(x) = \varphi(x - e)$$

Verifichiamo che è una derivazione:

$$\begin{aligned}
\xi_A(\varphi)(xy) = \varphi(xy - e) = \varphi(x(y - e) + (x - e)) \\
= x\varphi(y - e) + \varphi(x - e) = x\xi_A(\varphi)(y) + \xi_A(\varphi)x
\end{aligned}$$

Bisogna mostrare che le mappe sono una l'inversa dell'altra e che sono equivalenze naturali. □

Ora che abbiamo conosciuto le derivazioni vediamo un loro sottogruppo:

Definizione 4.79. $\mathrm{IDer}(G, A)$ è il sottogruppo di $\mathrm{Der}(G, A)$ dato dalle *derivazioni interne* d_a (al variare di $a \in A$) definite come

$$d_a(x) = (x - e)a$$

Mostriamo intanto che d_a è effettivamente una derivazione:

$$d_a(xy) = (xy - e)a = [x(y - e) + (x - e)]a = xd_a(y) + d_a(x)$$

Come ci si aspetta, $d_a + d_b = d_{a+b}$, e quindi questo è effettivamente un sottogruppo. Ora siamo finalmente pronti per calcolare $H^1(G, A)$.

Ricordiamo che $H^1(G, A) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Invece che una risoluzione, questa volta scegliamo una presentazione proiettiva di $\mathbb{Z}$ (come $\mathbb{Z}[G]$-modulo, ovviamente). Questa è data dall'augmentazione:

$$0 \to IG \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

dove $\mathbb{Z}[G]$ è proiettivo perché libero. Applichiamo $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A)$ e otteniamo

$$\mathrm{Hom}(\mathbb{Z}, A) \to \mathrm{Hom}(\mathbb{Z}[G], A) \xrightarrow{i^*} \mathrm{Hom}(IG, A)$$

Combinando quando visto abbiamo quindi

$$\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A) = \mathrm{Coker}\, i^* \cong {\mathrm{Hom}(IG, A)}\big/{i^*(\mathrm{Hom}(\mathbb{Z}[G], A))} \simeq {\mathrm{Der}(G, A)}\big/{H}$$

Bisogna studiare l'ultimo quoziente. Per definizione, gli elementi del sottomodulo $i^*(\mathrm{Hom}(\mathbb{Z}[G], A))$ sono della forma $\psi \circ i$, con $\psi \in \mathrm{Hom}(\mathbb{Z}[G], A)$. 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 $\psi(e) = a$. Da cui

$$\psi(x - e) = \psi((x - e)e) = (x - e)\psi(e) = (x - e)a = d_a(x)$$

e quindi $H = \langle d_a \mid a \in A \rangle = \mathrm{IDer}(G, A)$; abbiamo così caratterizzato l'H^1. Vediamo qualche esempio concreto.
Sia $C_m = \langle x \rangle$ il gruppo ciclico di ordine m e sia $A = (\mathbb{Z}/2\mathbb{Z})^m$, dove il generatore x agisce come

$$x(a_1, \ldots, a_m) = (a_m, a_1, \ldots, a_{m-1})$$

Vediamo chi è $H^1(C_m, (\mathbb{Z}/2\mathbb{Z})^m)$ passando per le derivazioni. Ci tocca quindi capire come sono fatte le derivazioni in $\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m)$. Sappiamo già che $d(e) = 0$. Se $d(x) = (a_1, \ldots, a_m)$, allora $d(x^2) = xd(x) + d(x)$, e similmente $d(x^3) = x^2d(x) + xd(x) + d(x)$ 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

$$(a_1, \ldots, a_m) + (a_m, a_1 \ldots, a_{m-1}) + (a_{m-1}, \ldots, a_{m-2}) + \cdots + (a_2, \ldots, a_1) = 0$$

Le derivazioni sono quindi oggetti che mappano $d(x) = (a_1, \ldots, a_m)$ con $\sum a_i = 0$, e possiamo scrivere quindi

$$\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m) = \mathrm{Ker}(e + x + x^2 + \ldots, +x^{m-1})$$

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

$$\mathrm{IDer} = \mathrm{Im}(x - e)$$

Ne segue che

$$\mathrm{Der}(C_m, (\mathbb{Z}/2\mathbb{Z})^m) \big/ \mathrm{IDer}(C_m, (\mathbb{Z}/2\mathbb{Z})^m) \cong \mathrm{Ker}(e + x + \ldots + x^{m-1}) \big/ \mathrm{Im}(x - e)$$

Queste due mappe sono mappe di 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

$$\begin{pmatrix} -1 & 0 & \ldots & 0 & 1 \\ 1 & -1 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & -1 & 0 \\ 0 & 0 & \ldots & 1 & -1 \end{pmatrix}$$

che ha rango $m - 1$. D'altra parte $\dim \mathrm{Ker}(e + x + \ldots + x^{-1}) \leq m - 1$, per cui[15] $H^1(C_m, (\mathbb{Z}/2\mathbb{Z})^m) = 0$.
Consideriamo ora $C_2 = \{e, x\}$ 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 $\mathrm{IDer}(C_2, \mathbb{Z})$: una derivazione interna d_n si può identificare col suo valore in x, e 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 $H^1(C_2, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Una risoluzione di proiettiva di $\mathbb{Z}$ come C_m-modulo Per lo studio dei gruppi di omologia e coomologia di ordine più alto, abbiamo però necessità di trovare qualche risoluzione. Presentiamo una risoluzione proiettiva comoda di $\mathbb{Z}$ visto come C_m-modulo banale. Questa è

[15] "Uno degli zeri più faticosi che abbiamo calcolato durante il corso."

$$\cdots \longrightarrow \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{T} \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{T} \mathbb{Z}[C_m] \longrightarrow 0$$
$$\mathbb{Z}[C_m] \xrightarrow{\epsilon} \mathbb{Z}$$

dove $T(e) = x - e$ e $N(e) = e + x + \ldots + x^{m-1}$. È facile vedere che in ϵ c'è l'esattezza (è l'augmentazione) e $N \circ T$ e $T \circ N$ sono nulle, e che quindi è un complesso. Mostriamo ora l'esattezza; da questo seguirà che se uno degli H_i o H^i è non nullo ce ne sono infiniti non nulli. Quindi non esistono risoluzioni proiettive di $\mathbb{Z}$ come $\mathbb{Z}[C_m]$-modulo finite, altrimenti gli H_i ed H^i da un certo punto in poi sarebbero tutti nulli.
Sia $y \in \operatorname{Ker} T$, e scrivendo $y = \sum a_h x^h$, abbiamo

$$0 = T(y) = \Big(\sum_{h=0}^{m-1} a_h x^h\Big)(x-1)$$

per essere 0 allora deve essere $0 = \sum 0x^h$, per cui per com'è fatta la somma (è telescopica) deve valere $a_0 = a_1 = \ldots = a_m = A$. Allora $y = (1 + x + \ldots + x^{m-1})A$ e $y \in \operatorname{Im} N$. L'altra inclusione ce l'avevamo già e quindi $\operatorname{Ker} T = \operatorname{Im} N$.
Calcoliamo ora i gruppi di omologia $H_m(C_m, \mathbb{Z}) = \operatorname{Tor}_n^{\mathbb{Z}[C_m]}(\mathbb{Z}, \mathbb{Z})$. Tensorizzando la successione otteniamo

$$\cdots \xrightarrow{T\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \xrightarrow{N\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \xrightarrow{T\otimes \mathrm{id}} \mathbb{Z}[C_m] \otimes_{\mathbb{Z}[C_m]} \mathbb{Z} \to 0$$

A meno di isomorfismo, questa sarebbe $\cdots \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z} \to 0$, ma bisogna esplicitare le mappe. Dato che $T(1) = x - 1$ e che $\mathbb{Z}$ ha la struttura di $\mathbb{Z}[C_m]$ modulo banale, allora $(x-1)n$ è sempre 0, per cui una mappa l'abbiamo identificata. Analogamente si vede che l'altra mappa è la moltiplicazione per m, quindi in definitiva abbiamo

$$\cdots \to \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0$$

E possiamo finalmente calcolare l'omologia:

- $H_0(C_m, \mathbb{Z}) = \mathbb{Z}$
- $H_{2k+1}(C_m, \mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$
- $H_{2k}(C_m, \mathbb{Z}) = 0$.

Dunque tutti i gruppi di omologia dispari sono non nulli.

Per l'omologia la situazione è analoga ma a ruoli invertiti.

Bar Resolution Omogenea Dopo quanto visto è evidente che per calcolare la coomologia di gruppi ci interessa avere risoluzioni proiettive di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo banale. Ce ne sono alcune che, sebbene molto grandi, sono disponibili sempre. Una si chiama *bar resolution omogenea*, e la presentiamo così:

$$B_n \xrightarrow{\partial_n} B_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{} 0$$
$$B_0 \xrightarrow{\varepsilon} \mathbb{Z}$$

dove B_n è lo $\mathbb{Z}[G]$-modulo dato da tutte le $n+1$-uple $(y_0, \dots, y_n)$ (con gli $y_i \in G$) tali che $\forall y \in G$ valga $y(y_0, \dots, y_n) = (yy_0, \dots, yy_n)$. Il motivo per cui B_n è proiettivo è che in realtà è lo $\mathbb{Z}[G]$-modulo libero con base $(1, y_1, \dots, y_n)$. Chi è il differenziale? Lo definiamo 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 vale $\partial_n \circ \partial_{n-1} = 0$. Mostriamo che la successione è esatta. Guardiamo il complesso come complesso di $\mathbb{Z}$-moduli, cioè di gruppi abeliani. Per mostrare che è esatto lo mandiamo in sé stesso con l'identità e la mappa nulla e mostriamo che sono omotope, per cui indurranno la stessa mappa in omologia $\mathrm{id}^* = 0^*$, e l'unico modo in cui questo può essere vero è che $H_n = 0$ (chiaramente intendiamo per ogni $n \geq 1$; l'H_0 sarà $\mathbb{Z}$).

$$\begin{array}{ccccccccc}
B_{n+1} & \xrightarrow{\partial_{n+1}} & B_n & \xrightarrow{\partial_n} & \cdots & \xrightarrow{\partial_{n-1}} & B_1 & \xrightarrow{\partial_{n-2}} & 0 \\
 & \swarrow{\scriptstyle \Sigma_n} & \downarrow{\scriptstyle \mathrm{id}-0} & \swarrow{\scriptstyle \Sigma_{n-1}} & & & \downarrow{\scriptstyle \mathrm{id}-0} & & \\
B_{n+1} & \xrightarrow[\partial'_{n+1}]{} & B_n & \xrightarrow[\partial'_n]{} & \cdots & \xrightarrow[\partial'_{n-1}]{} & B_1 & \xrightarrow[\partial'_{n-1}]{} & 0
\end{array}$$

Vogliamo Σ tale che $\partial_{n+1} \circ \Sigma_n + \Sigma_{n-1} \circ \partial_n = \mathrm{id} - 0$. Chiaramente il -0 ce lo possiamo dimenticare, comunque un'omotopia che funziona è

$$\Sigma_n((y_0, \dots, y_n)) = (1, y_0, \dots, y_n)$$

con $\Sigma_{-1}(1) = 1$. Il difetto di questa risoluzione è che è parecchio grande.

Bar Resolution Non Omogenea La Bar Resolution Non Omogenea è invece

$$B'_n \xrightarrow{\partial'_n} B'_{n-1} \xrightarrow{\partial'_{n-1}} \cdots \xrightarrow{\partial'_2} B'_1 \xrightarrow{\partial'_1} B'_0 \longrightarrow 0$$
$$\searrow \quad \nearrow$$
$$\mathbb{Z}$$

dove B'_n è lo $\mathbb{Z}[G]$-modulo libero $[x_1 \mid x_2 \mid \ldots \mid x_n]$, con gli $x_i \in G$, e B'_0 è lo $\mathbb{Z}[G]$-modulo con base $[]$, dove $\epsilon'([]) = 1$. Inoltre

$$\epsilon'(g[]) = g\epsilon'([1]) = g \cdot 1 = 1$$

Le mappe di bordo sono fatte in questa maniera:

$$\delta'_n([x_1 \mid x_2 \mid \ldots \mid x_n]) = x_1[x_2, \ldots, x_n] + \Big(\sum_{i=1}^{n-1}(-1)^i[x_1 \mid \ldots \mid x_i x_{i+1} \mid \ldots \mid x_n]\Big) + (-1)^n[x_1, \ldots, x_{n-1}]$$

Fra i due complessi $\{B_j\}$ e $\{B'_j\}$ c'è un isomorfismo di complessi $\varphi\colon B \to B'$

$$\begin{array}{ccccccccc} B_{n+1} & \xrightarrow{\partial_{n+1}} & B_n & \xrightarrow{\partial_n} & \cdots & \xrightarrow{\partial_{n-1}} & B_1 & \xrightarrow{\partial_{n-2}} & 0 \\ \downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi_n} & & & & \downarrow{\scriptstyle \varphi_1} & & \\ B'_{n+1} & \xrightarrow[\partial_{n+1}]{} & B'_n & \xrightarrow[\partial_n]{} & \cdots & \xrightarrow[\partial_{n-1}]{} & B'_1 & \xrightarrow[\partial_{n-1}]{} & 0 \end{array}$$

dato dalle

$$\varphi_n(1, y_1, \ldots, y_n) = [y_1 \mid y_1^{-1}y_2 \mid y_2^{-1}y_3 \mid \ldots \mid y_{n-1}^{-1}y_n]$$

Facciamo un po' di pratica con questo differenziale: ad esempio

$$(1, y_1, y_2) \xrightarrow{\varphi_2} [y_1 \mid y_1^{-1}y_2] \xrightarrow{\partial'_2} y_1[y_1^{-1}y_2] - [y_1 y_1^{-1} y_2] + [y_1] = y_1[y_1^{-1}y_2] - [y_2] + [y_1]$$

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

$$\varphi_1(y_1, y_2) = \varphi_1(y_1(1, y_1^{-1}y_2)) = y_1\varphi_1((1, y_1^{-1}y_2)) = y_1[y_1^{-1}y_2]$$

e altrettanto facilmente si vede $\varphi_1((1, y_2)) = [y_2]$ e $\varphi_1((1, y_1)) = [y_1]$, per cui le φ_i fanno commutare il diagramma. L'inversa di φ è $\psi\colon B' \to B$ data dalle

$$\psi_n([x_1, \ldots, x_n]) = (1, x_1, x_1x_2, x_1x_2x_3, \ldots, x_1, x_2, \ldots, x_n)$$

Dato che sappiamo già che la bar resolution omogenea è aciclica, tramite l'isomorfismo esibito ne segue che anche la bar resolution non omogenea è aciclica. Altrimenti si può considerare direttamente l'omotopia $\bar{\Delta}_{-1}(1) = []$ e $\bar{\Delta}_n(x[x_1, \ldots, x_n]) = [x \mid x_1 \mid \ldots \mid x_n]$.

La bar resolution non omogenea ci permette di calcolare l' $H^2(G, A)$.

Esercizio 4.80. Dati G e A individuare i 2-cocicli, ossia $\operatorname{Ker}\partial_3^*$, all'interno del complesso

$$0 \to \operatorname{Hom}(B'_0, A) \to \operatorname{Hom}(B'_1, A) \to \operatorname{Hom}(B'_2, A) \xrightarrow{\partial_2^*} \operatorname{Hom}(B'_3, A)$$

Soluzione. Sia $\in \operatorname{Hom}_{\mathbb{Z}[G]}(B'_2, A)$. La mappa f è decisa dai valori $f([x, y])$. Dunque associamo ad f una funzione, che chiamiamo ancora f, da $G \times G$ in A, definita come

$$f\colon G \times G \to A \qquad f((x, y)) = f([x, y])$$

Vediamo chi è $\operatorname{Ker}\partial_3^*$. Se f ci appartiene vuol dire che $\partial_3^* f = 0$, e quindi è nulla su ogni elemento, per cui, ricordandosi chi è il differenziale della bar resolution non omogenea, abbiamo

$$\begin{aligned} 0 = \delta_3^* f([x, y, z]) &= f \circ \partial_3([x, y, z]) \\ &= f\big(x[y, z] + (-[xy, z] + [x, yz]) - [x, y]\big) \\ &= xf([y, z]) - f([xy, z]) + f([x, yz]) - f([x, y]) \end{aligned}$$

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

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

Più in generale possiamo associare al un complesso i morfismi nella categoria degli insiemi come con le parentesi graffe qui:

$$0 \to \underbrace{\operatorname{Hom}_{\mathbb{Z}[G]}(B'_0, A)}_{F\colon \{*\} \to A} \to \underbrace{\operatorname{Hom}_{\mathbb{Z}[G]}(B'_1, A)}_{F\colon G \to A} \to \underbrace{\operatorname{Hom}_{\mathbb{Z}[G]}(B'_2, A)}_{F\colon G \times G \to A} \to \cdots$$

e come visto qui sopra il differenziale si "traduce" a livello insiemistico, dove ∂_n^* si legge come

$$\begin{aligned} \partial_n^* f(x_1, \ldots, x_{n+1}) = x_1 f(x_2, \ldots, x_{n+1}) &+ \sum_{i=1}^{n-1} (-1)^i f(\ldots, x_i x_{i+1}, \ldots) \\ &+ (-1)^n f(x_1, \ldots, x_n) \end{aligned}$$

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. □

Ora capiamo finalmente cosa rappresenta/calcola $H^2(G, A)$. Sia G un gruppo e A un G-modulo. Possiamo parlare del prodotto semidiretto $A \rtimes G$. Infatti A è un gruppo abeliano, e per definizione di G-modulo abbiamo un

morfismo fra $\varphi\colon G \to \mathrm{Aut}(A)$ che mappa g in $\varphi_g\colon a \mapsto ga$. Infatti 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

$$A \rtimes G = \{(a,g) \mid a \in G, g \in G\} \qquad (a,g)(a_1,g_1) = (a + g \cdot a_1, gg_1)$$

Ricordiamo che

$$(a,g)^{-1} = -(g^{-1}a, g^{-1})$$

Abbiamo la successione esatta di gruppi

$$1 \to A \xrightarrow{i} A \rtimes G \xrightarrow{\pi} G \to 1$$

Consideriamo adesso G, A un G-modulo e

$$1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

Questa è una successione esatta di gruppi, con A abeliano e, dato che $i(A) = \mathrm{Ker}\, p$, abbiamo che $i(A)$ è un sottogruppo normale di E. Prendiamo ora una *sezione*, cioè un *funzione*[16] $s\colon G \to E$ tale che $p \circ s = \mathrm{id}_G$. Descriviamo un'azione di G su $i(A)$ come

$$g \cdot i(a) \equiv s(g)i(a)s(g)^{-1}$$

che funziona perché iA è normale. Questa è un'azione, cioè $(gh) \cdot ia = g \cdot (h \cdot ia)$. Vediamo è che l'azione non dipende dalla scelta della sezione s. Se t è un'altra sezione, abbiamo $p(s(g)) = p(t(g))$, per cui $p(t(g)^{-1}s(g)) = 1$. Allora $t(g)^{-1}s(g) \in \mathrm{Ker}\, p = \mathrm{Im}\, i$ e quindi $t(g)^{-1}s(g) = i(a')$ per un certo a'. Dunque vale $s(g) = t(g)i(a')$ e

$$s(g)i(a)s(g)^{-1} = t(g)\underbrace{i(a')i(a)(ia')^{-1}}_{=ia}t(g)^{-1} = t(g)i(a)t(g)^{-1}$$

dove il passaggio con la parentesi è possibile grazie all'abelianità di $i(A)$. Possiamo enunciare ora che

Definizione 4.81. 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.

Osservazione 4.82. La successione esatta

$$1 \to A \to A \rtimes G \to G \to 1$$

è un'estensione.

[16] Non omomorfismo.

Fra due estensioni c'è un concetto di isomorfismo, lo "stesso" che per le estensioni di moduli: se esiste ψ che fa commutare

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Enunciamo il seguente, senza dimostrazione

Teorema 4.83. $H^2(G, A)$ è in bigezione con le classi di equivalenza di estensioni di G tramite A.

Concludiamo con due note:

1. Se G agisce su A banalmente, cioè se $s(g)i(a)s(g)^{-1} = ia$, questo corrisponde alle estensioni "centrali", cioè $i(A) \subset Z(E)$.

2. Consideriamo $\mathrm{Ext}^1(A, B)$, come $\mathbb{Z}$-moduli. Allora A, B sono gruppi abeliani; presa un'estensione, notiamo che è per forza centrale per abelianità, e chiamando $G = A$ si ottiene

   $$0 \to B \to E \to \underbrace{A}_{G} \to 0$$

   e pensare a B come A-modulo banale. A questo punto questa estensione è una di quelle che abbiamo appena presentato. Questo Ext^1 esaurisce tutte quelle che saltano fuori da H^2? No!

Esempio 4.84 (Perfido)**.** Consideriamo

$$0 \to \underbrace{\{\pm 1\}}_{B} \to Q_8 \to \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{A} \to 0$$

dove Q_8 sono i quaternioni e si considera A che agisce banalmente su B.

Questa è "conteggiata" da $H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2)$, ma non da Ext^1 (non è abeliana).