Appunti del corso
Istituzioni di algebra

Riccardo Zanotto, Andrea Gallese

7 ottobre 2019

Indice

Indice ii

1 Algebra commutativa **1**

1.1 Estensioni intere 1
1.2 Dimensione 3
1.3 Azione di Galois 4
1.4 Valutazioni e completamenti 5

2 Algebra omologica **6**

2.1 E-strutture e H^1 di gruppi 6
2.2 Categorie abeliane e complessi 8
2.3 Coomologia di gruppi 10
2.4 Gruppo di Brauer 12
2.5 Costruzione dei funtori derivati 16

Capitolo 1

Algebra commutativa

Lemma 1.0.1. *Sia* $\varphi : A \to B$ *di anelli, e* $\mathfrak{p} \subset A$ *ideale primo. Allora esiste* $\mathfrak{q} \subset B$ *primo con* $\mathfrak{p} = \mathfrak{q}^c$ *se e solo se* $\mathfrak{p} = \mathfrak{p}^{ce}$.

Lemma 1.0.2. *Sia* A *un* PID*: un modulo* M *è piatto se e solo è libero da torsione.*

1.1 Estensioni intere

Definizione 1.1.1. Dati $A \subset B$ anelli, $b \in B$ si dice *intero su* A se esiste un polinomio monico $f \in A[t]$ tale che $f(b) = 0$.
Se $I \subset A$ è un ideale, diciamo che b è intero su I se esiste $f \in I[t]$ monico che annulla b.
Se $f : A \to B$ è morfismo di anelli con 1, $I \subset A$, diciamo che b è intero su I se lo è su I^e.

Proposizione 1.1.2 (Funzionamento Tecnico degli Interi)**.** *Siano* $A \subset B$, $b \in B$*. Sono equivalenti:*

i. *b è intero su A.*

ii. *$A[b]$ è finitamente generato come A-modulo.*

iii. *$\exists C$ anello tale che $A[b] \subset C$ e C è fin. gen. come A-modulo.*

iv. *$\exists M$ un $A[b]$-modulo fedele, fin. gen. come A-modulo.*

Definizione 1.1.3. Siano $A \subset B$.

- Definiamo $\overline{A}^B = \{b \in B \mid b \text{ è intero su } A\}$ la *chiusura integrale* di A in B.
- Diciamo che $A \subset B$ è *intera* se vale $\overline{A}^B = B$.
- Diciamo che $A \subset B$ è *finita* se B è un A-modulo finitamente generato.

Proposizione 1.1.4.

- *Se $b_1, \dots, b_n \in B$ sono interi su A, allora $A[b_1, \dots, b_n]$ è fin. gen. come A-modulo.*
- *$\overline{A}^B$ è un sottoanello di B.*
- *Un'estensione finita è anche intera.*

- *Se $A \subset B \subset C$ con $A \subset B, B \subset C$ finite, allora anche $A \subset C$ è finita.*
- *Se $A \subset B \subset C$ con $A \subset B, B \subset C$ intere, allora anche $A \subset C$ è intera.*

Lemma 1.1.5. *Sia $A \subset B$ intera, $I \subset A$ ideale. Detto $\overline{I}^B = \{b \in B \mid b$ è intero su $I\}$, vale $\overline{I}^B = \sqrt{I^e}$.*

Proposizione 1.1.6. *Sia $A \subset B$ intera, J ideale di B, S parte moltiplicativa di A. Abbiamo che:*

- *${}^{A}\!/_{J^c} \subset {}^{B}\!/_{J}$ è intera;*
- $\overline{S^{-1}A}^{S^{-1}B} = S^{-1}(\overline{A}^B)$.

Definizione 1.1.7 (Normale)**.** Se A è un dominio. Si dice che A è *normale* se è integralmente chiuso del suo campo dei quozienti: $\overline{A}^K = A$, dove K sarà il campo dei quozienti.

Proposizione 1.1.8. *Ogni* UFD*è normale.*

Teorema 1.1.9 (Comodità dei Normali)**.** *Sia A dominio normale, K il campo dei quozienti; sia $K \subset L$ un'estensione algebrica; sia $I \subset A$ un ideale. Dato un $x \in L$ vale $x \in \overline{I}^L \iff \mu_x(t) \in \sqrt{I}[t]$. In particolare*

$$x \in \overline{A}^L \iff \mu_x(t) \in A[t].$$

Esempio 1.1.10. Se $A = \mathbb{Z}, K = \mathbb{Q}, L = \mathbb{Q}[\sqrt{d}]$, allora $\overline{A}^L = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}$

Lemma 1.1.11. *Sia $A \subset B$ intera di domini. Allora A è un campo se e solo se B è un campo.*

Corollario 1.1.12. *Sia $A \subset B$ intera, $\mathfrak{p} \subset B$ primo. Allora $\mathfrak{p}$ è massimale se e solo se $\mathfrak{p}^c$ è massimale.*

Corollario 1.1.13. *Sia $A \subset B$ intera, $\mathfrak{p} \subset \mathfrak{q} \subset B$ ideali primi. Se $\mathfrak{p}^c = \mathfrak{q}^c$ allora $\mathfrak{p} = \mathfrak{q}$.*

Teorema 1.1.14 (Lying over)**.** *Sia $A \subset B$ intera. Allora $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ è surgettiva.*

Definizione 1.1.15. Sia $A \subset B$, e $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset A$ ideali primi.

- Si dice che vale il *going up* se dato $\mathfrak{q}_1 \subset B$ con $\mathfrak{q}_1^c = \mathfrak{p}_1$, allora esiste $\mathfrak{q}_2 \supset \mathfrak{q}_1$ con $\mathfrak{q}_2^c = \mathfrak{p}_2$.
- Si dice che vale il *going down* se dato $\mathfrak{q}_2 \subset B$ con $\mathfrak{q}_2^c = \mathfrak{p}_2$, allora esiste $\mathfrak{q}_1 \subset \mathfrak{q}_2$ con $\mathfrak{q}_1^c = \mathfrak{p}_1$.

Teorema 1.1.16 (Going Down)**.** *Sia $A \subset B$.*

- *Se l'estensione è intera, allora $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ è chiusa.*
- *Se $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ è chiusa, allora vale il going up.*

Proposizione 1.1.17. *Sia $A \subset B$; se vale il going up e B è noetheriano, allora $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ è chiusa.*

Lemma 1.1.18 (degli Aperti)**.** *Sia $f : A \to B$, e $\varphi : Y = \operatorname{Spec} B \to \operatorname{Spec} A = X$; dato $\mathfrak{q} \in Y$, definiamo $Y_\mathfrak{q} = \operatorname{Spec} B_\mathfrak{q} = \{r \in Y \mid r \subset \mathfrak{q}\}$. Allora*

1. $Y_\mathfrak{q} = \bigcap_{\alpha \notin \mathfrak{q}} Y_\alpha$
2. $\varphi(Y_\mathfrak{q}) = \bigcap_{\alpha \notin \mathfrak{q}} \varphi(Y_\alpha)$

Teorema 1.1.19 (Going Down)**.** *Sia $f : A \to B$ e $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$. Se φ è aperta, allora vale il going down per f.*

Teorema 1.1.20. *Sia $A \subset B$ intera con A, B domini, e A normale. Allora $\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ è aperta.*

Proposizione 1.1.21. *Sia $f : A \to B$, e supponiamo che valga il going down; se A è noetheriano, allora φ è aperta.*

1.2 Dimensione

Definizione 1.2.1. La *dimensione* di un anello A è la massima lunghezza di una catena di ideali primi: se $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$, allora diciamo che $\dim A \geq n$.

Proposizione 1.2.2. *Se $A \subset B$ è intera, allora* $\dim A = \dim B$.

Teorema 1.2.3. *Sia A una k-algebra fin. gen, $A = k[y_1, \dots, y_n]$ (le y_i sono generatori come algebra); allora esistono $x_1, \dots, x_m \in A$ algebricamente indipendenti tali che $k[x_1, \dots, x_m] \subset A$ è intera.*
Inoltre se $y_1, \dots, y_n$ sono algebricamente dipendenti, allora $m < n$ e per k infinito le x_i possono essere scelte come combinazioni lineari delle y_j.

Proposizione 1.2.4. *Vale* $\dim k[x_1, \dots, x_n] = \dim k[x_1, \dots, x_n]_f = n$ *per ogni $f \in k[x_1, \dots, x_n]$.*

Definizione 1.2.5. Se A è un dominio e $k \subset A$, una *base di trascendenza* di A su k è un insieme massimale di elementi algebricamente indipendenti

Lemma 1.2.6. *Se x_α è base di trascendenza di A su k, allora l'estensione $k(x_\alpha) \subset \mathbb{Q}(A)$ è algebrica.*

Teorema 1.2.7. *Tutte le basi di trascendenza hanno la stessa cardinalità.*

Corollario 1.2.8. *Se A è una k-algebra fin. gen. e un dominio, allora* $\dim A = \operatorname{Tr}\deg_k A$.

Definizione 1.2.9. Sia $\mathfrak{p} \subset A$ un ideale primo; definiamo

- l'*altezza* $\operatorname{ht}(\mathfrak{p}) = \dim A_\mathfrak{p} = \max\{n \mid \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n = \mathfrak{p}\}$
- la *coaltezza* $\operatorname{coht}(\mathfrak{p}) = \dim A/\mathfrak{p} = \max\{n \mid \mathfrak{p} = \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n\}$

Lemma 1.2.10. *Sia A un dominio e una k-algebra fin. gen; sia $\mathfrak{p}$ un primo di altezza 1. Allora* $\dim A/\mathfrak{p} = \dim A - 1$.

Teorema 1.2.11. *Sia A una k-algebra fin. gen. Allora*

1. *Se $\mathfrak{p} \in \operatorname{Spec} A$, allora* $\operatorname{ht}(\mathfrak{p}), \operatorname{coht}(\mathfrak{p}) < \infty$.
2. *Dati $\mathfrak{p} \subset \mathfrak{q}$ due primi, ogni catena massimale $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{q}$ ha lunghezza* $\operatorname{coht}(\mathfrak{p}) - \operatorname{coht}(\mathfrak{q})$.
3. *Se A è un dominio, $\mathfrak{p} \in \operatorname{Spec} A$, allora vale* $\dim A = \operatorname{ht}(\mathfrak{p}) + \operatorname{coht}(\mathfrak{p})$.

Cosa succede in dimensione bassa?

Teorema 1.2.12. *Sia A un anello. Allora A è artiniano se e solo se è noetheriano e* $\dim A = 0$.

Definizione 1.2.13 (Lunghezza)**.** La lunghezza di modulo M è limite superiore sulle lunghezze delle catene di sottomoduli:

$$l(M)\colon \{n \mid \exists M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n\}$$

Proposizione 1.2.14. *Se esiste una catena di sottomoduli massimale di lunghezza finita, allora sono tutte finite e della stessa lunghezza.*

Proposizione 1.2.15. *La lunghezza $l(M)$ è finita se e solo se M è artiniano e noetheriano.*

Teorema 1.2.16. *Se $A \subseteq B$ è finita, si trovano solo finiti primi di Q sopra ogni* $\mathfrak{p} \in \operatorname{Spec} A$.

1.3 Azione di Galois

Sia A un dominio normale, $K = \mathbb{Q}(A)$ e $L \supset K$ un'estensione di Galois con gruppo G; sia $B = \overline{A}^L$:

$$\begin{tikzcd} B \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\ A \arrow[r, dash] & K. \end{tikzcd}$$

Definiamo $Y = \operatorname{Spec} B$, $X = \operatorname{Spec} A$, $\varphi\colon Y \to X$; sia poi $Y_\mathfrak{p} = \varphi^{-1}(\mathfrak{p})$, cioè i primi di B che stanno sopra A (che non è lo stesso $Y_\mathfrak{p}$ di sopra!).

Osservazione. Se $b \in B$, allora $\sigma(b) \in B$ per ogni $\sigma \in G$.
Inoltre se $\mathfrak{q} \in Y_\mathfrak{p}$, allora $\sigma(\mathfrak{q}) \in Y_\mathfrak{p}$.

Teorema 1.3.1. *Il campo fissato dal gruppo di decomposizione $L^{G_\mathfrak{q}}$ è la più piccola estensione di K sopra cui $\mathfrak{q}L^{G_\mathfrak{q}}$ troviamo un unico primo.*

Teorema 1.3.2. *Il gruppo G agisce transitivamente sull'insieme $Y_\mathfrak{p}$.*

Definizione 1.3.3. Fissato un primo $\mathfrak{q} \in Y$, definiamo il *gruppo di decomposizione* $G_\mathfrak{q} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$.

Definizione 1.3.4. Se $\mathfrak{p} = \mathfrak{q}^c$, detto $S = A \setminus \mathfrak{p}$, otteniamo un'estensione di campi

$$k(\mathfrak{p}) = {}^{S^{-1}A}\!\big/_{S^{-1}\mathfrak{p}} \subset {}^{S^{-1}B}\!\big/_{S^{-1}\mathfrak{q}} = k(\mathfrak{q})$$

Proposizione 1.3.5. *$G_\mathfrak{q}$ agisce dunque su $k(\mathfrak{q})$ tenendo fisso $k(\mathfrak{p})$, e la mappa*

$$G_\mathfrak{q} \to \{\varphi : k(\mathfrak{q}) \to k(\mathfrak{q}) \mid \varphi|_{k(\mathfrak{p})} = \mathrm{id}\} = \operatorname{Gal}\left({}^{k(q)}\!\big/_{k(p)}\right)$$

è surgettiva.

Teorema 1.3.6. *Sia A è un dominio normale dimensione* $\dim A = 1$. *Chiamiamo e l'indice di ramificazione (il numero per cui $\mathfrak{p}B_\mathfrak{q} = \mathfrak{q}^e B_\mathfrak{q}$), f l'indice d'inerzia (il grado dell'estensione $[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]$) e r la cardinalità di $Y_\mathfrak{q}$. Si ha che*

$$[L : K] = mef.$$

Teorema 1.3.7 (Finitezza dell'estensione intera)**.** *Nel classico setup*

$$\begin{array}{ccc} B & \text{——} & L \\ | & & | \\ A & \text{——} & K, \end{array}$$

supporre K/L separabile e finita e A normale e noetheriano è sufficiente per concludere che l'estensione degli anelli degli interi $A \subseteq B$ è a sua volta finita.

1.4 Valutazioni e completamenti

Definizione 1.4.1. Sia k un campo; una mappa $v : k^* \to \mathbb{Q}$ si dice *valutazione* se rispetta

- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min(v(x), v(y))$

Data una valutazione si definisce $A = \{x \in k \mid v(x) \geq 0\}$ e $\mathfrak{m} = \{x \in k \mid v(x) > 0\}$ un ideale di A. La valutazione v si dice *discreta* se $\operatorname{Im} v = \mathbb{Z} \cdot q$ per qualche $q \neq 0$; in questo caso A è un DVR.

Proposizione 1.4.2. *Sia A l'anello appena definito. Allora*

- *A è anello locale con unico massimale $\mathfrak{m}$.*
- *Se v è discreta, allora A è noetheriano, $\dim A = 1$ e tutti gli ideali sono della forma (π^m) dove $v(\pi) = q$.*

Teorema 1.4.3. *Sia A un anello locale noetheriano, con $\dim A = 1$. Allora sono equivalenti:*

i. A è un DVR

ii. A è un dominio normale

iii. l'ideale massimale è principale

Osservazione. Nel caso valgano le condizioni sopra, allora $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Proposizione 1.4.4. *Sia $f \in \mathbb{C}[x, y]$ irriducibile, e $A = {}^{\mathbb{C}[x,y]}\!/_{(f)}$. Allora A è normale se e solo se $f = 0$ è una curva liscia, ovvero $\nabla f \neq 0$ nei punti in cui $f = 0$.*

Capitolo **2**

Algebra omologica

2.1 E-strutture e H^1 di gruppi

Lemma 2.1.1. *Sia $E \subset F$ finita di Galois con gruppo Γ; V un E-spazio vettoriale.*

1. *Detto $V_F = F \otimes_E V$, Γ agisce su V_F tramite $\gamma(\lambda \otimes v) = \gamma(\lambda) \otimes v$ per $v \in V$. Valgono allora*
   - $V_F^\Gamma = V$
   - $\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$ *per* $v \in V_F$
2. *Se W è un F spazio vettoriale, e Γ agisce su W in modo che $\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$, allora detto $W_0 = W^\Gamma$ valgono*
   - *W_0 è un E-spazio vettoriale*
   - *la mappa $F \otimes_E W_0 \to W$ che manda $\lambda \otimes v \mapsto \lambda v$ è un isomorfismo*

Teorema 2.1.2. *Sia $E \subset F$ un'estensione di Galois infinita. Allora*

$$\mathrm{Gal}\left({}^{F}\!\diagup_{E}\right) \cong \varprojlim_{[L:E]<\infty} \mathrm{Gal}\left({}^{L}\!\diagup_{E}\right)$$

Definizione 2.1.3. Data $E \subset F$ di Galois, un'azione di $\mathrm{Gal}\left({}^{F}\!\diagup_{E}\right)$ su uno spazio X è detta *continua* se $\forall x \in X\ \exists L \supset E$ finita di Galois, con $\mathrm{Gal}\left({}^{F}\!\diagup_{L}\right) \subset \operatorname{stab} x$

Lemma 2.1.4. *Sia $E \subset F$ di Galois infinita, V un F-spazio vettoriale; supponiamo che $\Gamma = \mathrm{Gal}\left({}^{F}\!\diagup_{E}\right)$ agisca in modo continuo su V e valga $\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$; allora valgono le conclusioni del punto 2 del lemma precedente, in particolare $V \cong F \otimes_E V^\Gamma$.*

Definizione 2.1.5. Sia $E \subset F$ estensione di Galois con gruppo Γ; siano A_0, B due E-algebre, e $R = F \otimes A_0 \cong F \otimes B$. Sia $\gamma_0 = \gamma \otimes_E \mathrm{id}_{A_0}$ l'azione di Γ estesa su R, e similmente γ_B.
Sia $c : \Gamma \to \mathrm{Aut}(R)$ dato da $c_\gamma = \gamma_B \cdot \gamma_A^{-1}$.

Proposizione 2.1.6.

- *Per ogni γ, c_γ è F-lineare, quindi ho definito $c : \Gamma \to \mathrm{Aut}_F(R)$*

- *Vale* $c_{\gamma\delta} = c_\gamma \circ^\gamma c_\delta$, *dove* ${}^\gamma\varphi = \gamma_0 \circ \varphi \circ \gamma_0^{-1}$

Definizione 2.1.7. Definiamo $Z^1(\Gamma, \mathrm{Aut}_F(R)) = \{c : \Gamma \to \mathrm{Aut}_F(R) \mid c_{\gamma\delta} = c_\gamma \circ^\gamma c_\delta\}$.
Se $c, c' \in Z^1$, diciamo che $c \sim c'$ se $\exists f \in \mathrm{Aut}_F R$ tale che $c'_\gamma = f \circ c_\gamma \circ^\gamma f^{-1}$.
Definiamo poi $H^1(\Gamma, \mathrm{Aut}_F(R)) = {Z^1(\Gamma, \mathrm{Aut}_F(R))}/{\sim}$

Teorema 2.1.8.

$$\{E\text{-strutture di } A\}/_{\text{isomorfismo}} \cong H^1(\Gamma, \mathrm{Aut}_F(R))$$

Sia ora G un gruppo che agisce sullo spazio X; sia Γ un gruppo che agisce su G conservando il prodotto e su X compatibilmente con G.

Definizione 2.1.9. Sia $Z^1(\Gamma, G) = \{c : \Gamma \to G \mid c_{\gamma\delta} = c_\gamma \cdot^\gamma c_\delta\}$.
Diciamo inoltre che $c \sim d$ se esiste $g \in G$ tale che $d_\gamma = g \cdot c_\gamma \cdot^\gamma (g^{-1})$.
Sia infine $H^1(\Gamma, G) = {Z^1(\Gamma, G)}/{\sim}$.

Proposizione 2.1.10. *Sia* $1 \to H \to G \to K \to 1$ *una successione esatta di gruppi su cui agisce* Γ *in modo compatibile con le mappe.*
Allora $1 \to H^\Gamma \to G^\Gamma \to K^\Gamma \to H^1(\Gamma, H) \to H^1(\Gamma, G) \to H^1(\Gamma, K)$ *è una successione esatta di insiemi puntati.*

Teorema 2.1.11 (Hilbert 90)**.** *Sia* $E \subset F$ *di Galois finita con gruppo* Γ*; sia* $G = \mathrm{GL}_n(F)$ *e* Γ *agisce su* G *coefficiente per coefficiente. Allora* $H^1(\Gamma, \mathrm{GL}_n(F)) = \{1\}$.

Corollario 2.1.12. *Anche* $H^1(\Gamma, \mathrm{SL}_n(F)) = \{1\}$.

Proposizione 2.1.13. *Sia* $x_0 \in X^\Gamma$ *e* $H = \mathrm{stab}_G\, x_0$*; supponiamo che* G *agisca transitivamente su* X*. Se* $H^1(\Gamma, G) = \{1\}$*, allora le orbite di* G^Γ *in* X^Γ *sono in bigezione con* $H^1(\Gamma, H)$.

2.2 Categorie, categorie abeliane e complessi

Lemma 2.2.1 (di Yoneda)**.** *Sia* $\mathcal{C}$ *una categoria piccola e* $F\colon \mathcal{C} \to \mathbf{Set}$ *un funtore controvariante nella categoria degli insiemi. Si ha una bigezione*

$$Nat(h_X,\, F) \leftrightarrow F(X).$$

Proposizione 2.2.2 (che fa impallidire anche Yoneda)**.** *I limiti sono coequalizzatori. Sia I un sistema proiettivo, allora* $\varprojlim F(i)$ *è isomorfo all'equalizzatore del diagramma*

$$\prod_i F(i) \underset{S}{\overset{T}{\rightrightarrows}} \prod_{\varphi: i \to j} F(j)_\varphi$$

dove otteniamo T ed S sfruttando la proprietà universale del prodotto per completare i diagrammi

$$\begin{tikzcd} \prod_i F(i) \arrow[r, dashed, "T"] \arrow[d, "\pi_b"] & \prod_{\varphi:i\to j} F(j)_\varphi \arrow[d, "\pi_{b\varphi}"] \\ F(b) \arrow[r, "\mathrm{id}"] & F(b)_\varphi, \end{tikzcd} \qquad \begin{tikzcd} \prod_i F(i) \arrow[r, dashed, "S"] \arrow[d, "\pi_a"] & \prod_{\varphi:i\to j} F(j)_\varphi \arrow[d, "\pi_{b\varphi}"] \\ F(a) \arrow[r, "\varphi"] & F(b)_\varphi. \end{tikzcd}$$

Definizione 2.2.3. Una categoria $\mathcal{C}$ si dice *additiva* se soddisfa le seguenti proprietà:

- $\forall X, Y \in \mathcal{C}$, l'insieme $\mathrm{Hom}(X, Y)$ è un gruppo abeliano
- La composizione di morfismi $\mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z)$ è bilineare
- Esiste un oggetto zero, cioè $0 \in \mathcal{C}$ tale che $\mathrm{Hom}(X, 0) = \mathrm{Hom}(0, X)$ sono il gruppo banale
- Dati $X, Y \in \mathcal{C}$ esiste il coprodotto $X \coprod Y$, definito dalla seguente proprietà universale:

$$\begin{tikzcd} & Z & \\ X \arrow[ur, "f"] \arrow[r, "i_X"'] & X \coprod Y \arrow[u, dashed] & Y \arrow[ul, "g"'] \arrow[l, "i_Y"] \end{tikzcd}$$

Proposizione 2.2.4. *In una categoria additiva, il coprodotto è isomorfo al prodotto, e si indica con $X \oplus Y$.*

Definizione 2.2.5. Fissata una mappa $\varphi : X \to Y$, diciamo che:

- $\ell : Z \to X$ è il *nucleo* di φ se $\varphi \circ \ell = 0$ e per ogni $\alpha : U \to X$ tale che $\varphi \circ \alpha = 0$, esiste un'unica $\tilde{\alpha} : U \to Z$ che faccia commutare

$$\begin{tikzcd} Z \arrow[r, "\ell"] & X \arrow[r, "\varphi"] & Y \\ & U \arrow[u, "\alpha"] \arrow[ul, dashed, "\tilde{\alpha}"] & \end{tikzcd}$$

- $m : Y \to Q$ è il *conucleo* di φ se $m \circ \varphi = 0$ e per ogni $\beta : Y \to U$ tale che $\beta \circ \varphi = 0$, esiste un'unica $\tilde{\beta} : Q \to U$ che faccia commutare

$$\begin{tikzcd} X \arrow[r, "\varphi"] & Y \arrow[r, "m"] \arrow[d, "\beta"] & Q \arrow[dl, dashed, "\tilde{\beta}"] \\ & U & \end{tikzcd}$$

Definizione 2.2.6. Una categoria additiva $\mathcal{C}$ è detta *abeliana* se per ogni mappa $\varphi : X \to Y$ esistono $\alpha = \ker \varphi$ e $\beta = \operatorname{coker} \varphi$, e inoltre $\operatorname{coker} \alpha \cong \ker \beta$ e questo oggetto si dice $\operatorname{Im} \varphi$.

$$\begin{tikzcd} K \arrow[r, "\alpha"] & X \arrow[r, "\varphi"] \arrow[d, "\pi"] & Y \arrow[r, "\beta"] & Q \\ & \operatorname{coker} \alpha \arrow[ur, dashed, "\psi"] \arrow[r, dashed, "\sim"', "\Phi"] & \ker \beta \arrow[u, "j"] & \end{tikzcd}$$

Proposizione 2.2.7. *In una categoria abeliana φ è un isomorfismo se e solo se* $\ker \varphi = 0$ *e* $\operatorname{coker} \varphi = 0$.

Definizione 2.2.8. La successione $X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$ si dice *esatta* in Y se $\psi\varphi = 0$ e vale $\operatorname{Im} \varphi \cong \ker \psi$ (o equivalentemente $\operatorname{Im} \psi \cong \operatorname{coker} \varphi$).

Proposizione 2.2.9. *In una categoria abeliana valgono lo snake lemma e il lemma dei 5.*

Lemma 2.2.10. *Nella categoria degli A-moduli il limite inverso $\varprojlim$ è esatto a sinistra.*

Teorema 2.2.11. *In realtà le categorie abeliane sono gli A-moduli...*

Complessi

Mettiamoci in una categoria abeliana $\mathcal{C}$.

Definizione 2.2.12. Una *complesso* $X^\bullet$ è una successione di oggetti e frecce

$$\dots \xrightarrow{\partial^{n-1}} X^n \xrightarrow{\partial^n} X^{n+1} \xrightarrow{\partial^{n+1}} \dots$$

tali che $\partial^{n+1} \circ \partial^n = 0$ per ogni $n \in \mathbb{Z}$.
Un *morfismo di complessi* $\varphi^\bullet : X^\bullet \to Y^\bullet$ è una successione di mappe $\varphi^n : X^n \to Y^n$ tali che tutti i quadrati commutino:

$$\begin{tikzcd} X^{n-1} \arrow[r, "\partial_X^{n-1}"] \arrow[d, "\varphi^{n-1}"] & X^n \arrow[r, "\partial_X^n"] \arrow[d, "\varphi^n"] & X^{n+1} \arrow[d, "\varphi^{n+1}"] \\ Y^{n-1} \arrow[r, "\partial_Y^{n-1}"] & Y^n \arrow[r, "\partial_Y^n"] & Y^{n+1} \end{tikzcd}$$

Possiamo allora considerare le categorie $\mathrm{Com}(\mathcal{C})$, $\mathrm{Com}^+(\mathcal{C})$ e $\mathrm{Com}^-(\mathcal{C})$ dei complessi (eventualmente limitati in una delle due direzioni).

Proposizione 2.2.13. *Le categorie* $\mathrm{Com}(\mathcal{C})$*,* $\mathrm{Com}^+(\mathcal{C})$ *e* $\mathrm{Com}^-(\mathcal{C})$ *sono abeliane.*

Definizione 2.2.14. Sia $X^\bullet$ un complesso; definiamo $Z^n(X) = \ker(\partial^n)$ e $B^n(X) = \mathrm{Im}(\partial^{n-1})$. Definiamo poi $H^n(X) = {Z^n(X)}/{B^n(X)}$ l'n-esimo gruppo di coomologia.

Proposizione 2.2.15. *Se* $\varphi^\bullet : X^\bullet \to Y^\bullet$ *è morfismo di complessi, otteniamo una successione di mappe* $H^n(\varphi) : H^n(X) \to H^n(Y)$*.*

Teorema 2.2.16. *Sia* $0 \to X^\bullet \xrightarrow{\varphi^\bullet} Y^\bullet \xrightarrow{\psi^\bullet} Z^\bullet \to 0$ *una successione esatta di complessi. Allora la successione*

$$H^n(X) \to H^n(Y) \to H^n(Z) \xrightarrow{\omega_n} H^{n+1}(X) \to H^{n+1}(Y) \to H^{n+1}(Z)$$

è esatta.

Definizione 2.2.17. Sia $\varphi : X^\bullet \to Y^\bullet$; diciamo che $\varphi \sim 0$ è *omotopa* a 0 se esistono delle mappe $h^n : X^n \to Y^{n-1}$ tali che $\varphi^n = \partial_Y^{n-1} \circ h^n + h^{n+1} \circ \partial_X^n$.

Proposizione 2.2.18. *Se* $\varphi \sim 0$*, allora vale* $H^n(\varphi) = 0$*; in particolare se vale* $\mathrm{id} \sim 0$*, allora il complesso è esatto.*

Definizione 2.2.19. Se $X^\bullet$ è un complesso, diciamo che il complesso $Y^\bullet$ è una *risoluzione iniettiva* di $X^\bullet$ se gli Y^n sono oggetti iniettivi ed esiste un morfismo di complessi $\varphi^\bullet : X^\bullet \to Y^\bullet$ che sia un isomorfismo in coomologia.

Definizione 2.2.20. Sia $A \in \mathcal{C}$ e $F : \mathcal{C} \to \mathcal{C}'$ un funtore additivo, esatto a sinistra.
Sia $I^\bullet$ una risoluzione iniettiva del complesso $\dots \to 0 \to A \to 0 \to \dots$.
Definiamo l'i-esimo funtore derivato come $R^iF(A) = H^i(FI^\bullet)$ l'i-esimo gruppo di coomologia del complesso $0 \to FI^0 \to FI^1 \to \dots$.

Osservazione. Verificheremo che la risoluzione iniettiva esiste, e che il funtore derivato non dipende dalla scelta della risoluzione iniettiva.

Definizione 2.2.21. Se $X^\bullet$ è un complesso, diciamo che il complesso $P^\bullet$ è una *risoluzione proiettiva* di $X^\bullet$ se i P^n sono oggetti iniettivi ed esiste un morfismo di complessi $\varphi^\bullet : P^\bullet \to X^\bullet$ che sia un isomorfismo in coomologia.

Definizione 2.2.22. Sia $A \in \mathcal{C}$ e $F : \mathcal{C} \to \mathcal{C}'$ un funtore controvariante, additivo, esatto a sinistra.
Sia $P^\bullet$ una risoluzione iniettiva del complesso $\ldots \to 0 \to A \to 0 \to \ldots$.
Definiamo l'i-esimo funtore derivato come $L^iF(A) = H^i(FP^\bullet)$ l'i-esimo gruppo di coomologia del complesso $0 \to FP^0 \to FP^1 \to \ldots$.

Definizione 2.2.23. Siano X, Y oggetti; siano F, G i funtori $F = \mathrm{Hom}(X, -)$ e $G = \mathrm{Hom}(-, Y)$.
Definiamo allora $\mathrm{Ext}^i(X, Y) = R^iF(Y)$ e $\underline{\mathrm{Ext}}^i(X, Y) = L^iG(X)$.

Esempio 2.2.24. Siano $m, n \in \mathbb{Z}$ e scriviamo $m = dm', n = dn'$ con $d = \gcd(m, n)$.
Allora $\underline{\mathrm{Ext}}^0(\mathbb{Z}/(m), \mathbb{Z}/(m)) \cong \underline{\mathrm{Ext}}^1(\mathbb{Z}/(m), \mathbb{Z}/(m)) \cong \mathbb{Z}/(d)$.

Proposizione 2.2.25. *Se X, Y sono oggetti, allora* $\mathrm{Ext}^i(X, Y) \cong \underline{\mathrm{Ext}}^i(X, Y)$.

2.3 Coomologia di gruppi

Sia G un gruppo e R un anello commutativo con unità. Lavoreremo nella categoria degli $R[G]$ moduli, dove $R[G] = \bigoplus_{g \in G} Re_g$.

Definizione 2.3.1. Sia M un $R[G]$-modulo; definiamo $F_1(M) = M^G = \mathrm{Hom}_{R[G]}(R, M)$ e $F_2(M) = M/\langle m - gm \rangle = R \otimes_{R[G]} M$.
Definiamo $H^n(G, M) = \mathrm{Ext}^n(R, M) = R^nF_1(M)$; sappiamo però che è isomorfo a $\underline{\mathrm{Ext}}^n(R, M)$, che è il funtore derivato di $\mathrm{Hom}_{R[G]}(-, M)$.
Inoltre $H_n(G, M) = \mathrm{Tor}_n(R, M)$ il funtore derivato di F_2.

Proposizione 2.3.2 (risoluzione libera di R)**.** *Siano $P^0 = R[G], P^{-1} = R[G \times G], P^{-2} = R[G \times G \times G], \ldots$; sia $\varepsilon : P^0 \to R$ data da $\varepsilon(g) = 1$.
Sia poi $\partial^{-n} : P^{-n} \to P^{-n+1}$ data da*

$$\partial^{-n}(e_{g_0,\ldots,g_n}) = \sum_{i=0}^{n} (-1)^i e_{g_0,\ldots,\hat{g}_i,\ldots,g_n}$$

Allora la successione $0 \leftarrow R \xleftarrow{\varepsilon} P^0 \xleftarrow{\partial^{-1}} P^{-1} \xleftarrow{\partial^{-2}} \ldots$ *è una risoluzione proiettiva di R.*

Proposizione 2.3.3. *La mappa* $\Phi_n : \mathrm{Hom}_{R[G]}(P^{-n}, M) \to \{f : G^n \to M\} =: C^n(G, M)$ *data da* $\Phi_n(\psi)(g_1, \ldots, g_n) = \psi(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n)$ *è un isomorfismo.*
Inoltre la mappa $\delta_C^n : C^n(G, M) \to C^{n+1}(G, M)$ *data da* $\delta_C^n f = \Phi_{n+1}((\Phi_n^{-1} f) \circ \partial^{-n})$ *ha la formula esplicita*

$$(\delta_C^n f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i \cdot g_{i+1}, \ldots, g_{n+1}) + (-1)^n f(g_1, \ldots, g_n)$$

Esempio 2.3.4. Osserviamo che $(\delta^0 f)(g) = gf(1) - f(1)$ e $(\delta^2 f)(g, h) = gf(h) - f(gh) + f(g)$, ovvero $Z^1(G, M) = \{f : G \to M \mid f(gh) = f(g) + gf(h)\}$ e perciò $H^1(G, M) = Z^1/\{g \mapsto gm - m\}$, che è esattamente la definizione data nel capitolo precedente con i cocicli c_γ.

Definizione 2.3.5. Sia $f : H \to G$ un omomorfismo di gruppi e M un G-modulo. Allora f^*M è un H-modulo tramite l'azione $h \cdot m = f(h)m$.
Inoltre f induce un morfismo di complessi $C^q(G, M) \to C^q(H, M)$, da cui si ottiene una mappa $Res^q : H^q(G, M) \to H^q(H, f^*M)$ in coomologia.

Definizione 2.3.6. Sia $f : H \to G$ un omomorfismo di gruppi e N un H-modulo.
Definiamo $\operatorname{Ind}_H^G N = R[G] \otimes_{R[H]} N$ che è un G-modulo tramite $g \cdot (x \otimes n) = xg \otimes n$.
Definiamo poi $\operatorname{coInd}_H^G N = \operatorname{Hom}_H(R[G], N)$, dove $R[G]$ è un H-modulo tramite l'azione $h \cdot g = gf(h^{-1})$. Questo ha una struttura di G-modulo con l'azione $(g \cdot \varphi)(x) = \varphi(g^{-1}x)$.

Proposizione 2.3.7. *Sia M un G-modulo e N un H-modulo, e $f : H \to G$. Allora valgono*

- $\operatorname{Hom}_H(N, f^*M) \cong \operatorname{Hom}_G(\operatorname{Ind}_H^G, M)$
- $\operatorname{Hom}_H(f^*M, N) \cong \operatorname{Hom}_G(M, \operatorname{coInd}_H^G N)$

Proposizione 2.3.8. *Siano F, G due funtori aggiunti tra due categorie $\mathcal{A}, \mathcal{B}$, ovvero tali che* $\operatorname{Hom}_{\mathcal{A}}(a, Gb) = \operatorname{Hom}_{\mathcal{B}}(Fa, b)$. *Allora valgono:*

- *F conserva i limiti diretti, è esatto a destra e manda proiettivi in proiettivi*
- *G conserva i limiti inversi, è esatto a sinistra e manda iniettivi in iniettivi*
- *Se $\mathcal{A}, \mathcal{B}$ sono abeliane, F e G sono additivi*

Teorema 2.3.9. *Sia $H < G$ e N un H-modulo. Allora*

- $H^i(G, \operatorname{coInd}_H^G N) = H^i(H, N)$
- $H_i(G, \operatorname{Ind}_H^G N) = H_i(H, N)$

Definizione 2.3.10. Dato G un gruppo, $H < G$ di indice finito, M un G-modulo, abbiamo le mappe:

- $i : M^G \to M^H$ la mappa di inclusione
- $N : M^H \to M^G$ la "norma": se $x_1, \ldots, x_n$ sono i rappresentanti di G/H, definiamo $N(m) = \sum x_i m$

Inoltre, se $0 \to M \to I_M^\bullet$ è risoluzione iniettiva come G-modulo, lo è anche come H-modulo.
Perciò le due mappe passano a mappe di complessi, e quindi in coomologia:

- $\operatorname{Res}^q : H^q(G, M) \to H^q(H, M)$
- $\operatorname{coRes}^q : H^q(H, M) \to H^q(G, M)$

Proposizione 2.3.11. *Sia $H < G$ di indice finito. Allora* $\operatorname{coRes}^q \circ \operatorname{Res}^q = [G : H] \operatorname{id}$.

Corollario 2.3.12. *Se G è finito, vale $\#G \cdot H^q(G, M) = 0$ per $q > 0$.*

2.4 Gruppo di Brauer

Consideriamo ora anelli A con unità, non necessariamente commutativi.

Algebre centrali semplici

Definizione 2.4.1. Sia M un A-modulo. Si dice *semplice* se $M \neq 0$ e non ha sottomoduli propri. M si dice *semisemplice* se $M = \sum_{S \subset M \text{ semplice}} S$.

Teorema 2.4.2. *Sia A anello con 1, M un A-modulo. Sono equivalenti*

1. *$\exists S_i \subset M$ semplici tali che $M = \bigoplus S_i$.*
2. *M è semisemplice.*
3. *Per ogni $N \subset M$ esiste un $P \subset M$ tale che $M = N \oplus P$.*

Osservazione. Sottomoduli e quozienti di semisemplici sono semisemplici.

Definizione 2.4.3. Un anello A si dice semisemplice se lo è come A-modulo sinistro.

Proposizione 2.4.4. *Sia A un anello. Sono equivalenti*

1. *A è semisemplice.*
2. *Ogni A-modulo è semisemplice.*
3. *Ogni A-modulo è proiettivo.*

Lemma 2.4.5 (Schur)**.** *Siano S, T moduli semplici. Allora*

- *Sia $\varphi : S \to T$. Si ha che $\varphi = 0$ oppure è un isomorfismo.*
- *$\mathrm{End}(S)$ è un corpo.*

Teorema 2.4.6 (Wedderburn)**.** *Sia A un anello semisemplice. Allora $A = \bigoplus_i \mathrm{Mat}_{n_i \times n_i}(D_i)$ con D_i corpi univocamente determinati.*

Proposizione 2.4.7. *Sia $E = \overline{E}$, e $D \supset E$ un corpo di dimensione finita con $E \subset Z(D)$. Allora $D = E$.*

Definizione 2.4.8. Una E-algebra A di dimensione finita si dice *centrale* se $Z(A) = E$; si dice *semplice* se A non contiene ideali bilateri non banali.

Proposizione 2.4.9. *Sia A una E-algebra di dimensione finita. Sono equivalenti*

1. *A è semplice.*
2. *$A = \mathrm{Mat}_{n \times n}(D)$ con D corpo tale che $E \subset Z(D)$.*

Corollario 2.4.10. *A è un'E-algebra centrale semplice se e solo se $A = \mathrm{Mat}_{n \times n}(D)$, con $Z(D) = E$.*

Lemma 2.4.11. *Sia V un E-spazio vettoriale, D un corpo E-centrale, $V_D = V \otimes_E D$ e $W \subset V_D$ un sottospazio vettoriale stabile per D a destra e a sinistra. Detto $W' = W \cap V$, vale $W = W' \otimes_E D$.*

Teorema 2.4.12. *Sia A una E-acs; $E \subset F$ estensione di campi. Allora $F \otimes_E A$ è una F-acs.*

Teorema 2.4.13. *Siano A, A' delle E-acs. Allora anche $A \otimes_E A'$ è una E-acs.*

Definizione 2.4.14. Sia A una E-acs. Diciamo che *spezza* su F se $A \otimes_E F = \mathrm{Mat}_{n \times n}(F)$

Teorema 2.4.15. *Sia A una E-acs. Allora esiste un'estensione di campi $E \subset F$ finita e separabile tale che A spezza su F.*

Definizione 2.4.16. Sia E un campo; definiamo il suo gruppo di Brauer come $\mathcal{A} = {\{E\text{-acs}\}}\diagup{\sim}$, dove $A \sim A'$ se sono algebre di matrici sullo stesso corpo. Questo è un gruppo, con l'operazione $[A] \cdot [A'] = [A \otimes A']$ ed elemento neutro $[E]$.

Osservazione. L'elemento inverso è l'algebra opposta, in quanto $A \otimes A^{op} = \mathrm{End}_E(A) = \mathrm{Mat}_{n\times n}(E)$.

Descrizione coomologica

Lemma 2.4.17. *Dato un campo F vale* $\mathrm{Aut}_F(\mathrm{Mat}_{n\times n}(F)) = PGL_n(F)$

Definizione 2.4.18. Sia $E \subset L$ finita di Galois con gruppo Γ. Definiamo i seguenti oggetti:

- $\mathcal{A}_L = \{[A] \in \mathcal{A} \mid A \text{ spezza su } L\}$
- $\mathcal{A}_n = \{A\ E\text{-acs} \mid \dim_E A = n^2\}/\text{isom.}$
- $\mathcal{A}_{n,L} = \{A\ E\text{-acs} \mid \dim_E A = n^2, A \text{ spezza su } L\}/\text{isom.}$

Osservazione. Le algebre $\mathcal{A}_{n,L}$ sono proprio le E-strutture di $\mathrm{Mat}_{n\times n}(L)$, pertanto c'è la corrispondenza biunivoca $\mathcal{A}_{n,L} \leftrightarrow H^1(\Gamma, PGL_n(L))$.

Definizione 2.4.19. Definiamo la mappa $\delta_{n,L} : \mathcal{A}_{n,L} \to H^2(\Gamma, L^*)$ tramite la successione lunga data da $1 \to L^* \to GL_n(L) \to PGL_n(L) \to 1$.

Lemma 2.4.20. *Siano $A \in \mathcal{A}_{n,L}$ e $A' \in \mathcal{A}_{m,L}$. Allora*

- $\delta_{nm}(A \otimes A') = \delta_n(A) \cdot \delta_m(A')$.
- *Se $[A] = [A']$ nel gruppo di Brauer, allora $\delta_n(A) = \delta_m(A')$.*
- *La mappa δ_k è surgettiva per $k = [L : E]$.*

Teorema 2.4.21. *Le mappe δ_n permettono di costruire l'isomorfismo di gruppi*

$$\mathcal{A}_L \cong H^2(\Gamma, L^*)$$

Corollario 2.4.22.

- *Se D è un corpo finito, allora è un campo.*
- *Il gruppo di Brauer di $\mathbb{R}$ è $\mathbb{Z}/(2)$, ovvero $\{\mathbb{R}, \mathbb{H}\}$*

Galois infinito

Definizione 2.4.23. In generale, sia G un gruppo, $H \trianglelefteq G$ e M un G-modulo. La mappa naturale $Inf^q : H^q\left({G}\diagup{H}, M^H\right) \to H^q(G, M)$ è detta *inflazione.*

Consideriamo ora $E \subset F$ di Galois con gruppo Γ; per ogni $E \subset L$ finita di Galois indichiamo $\Sigma_L = \mathrm{Gal}\left({F}\diagup{L}\right)$, $\Gamma_L = \mathrm{Gal}\left({L}\diagup{E}\right) = {\Gamma}\diagup{\Sigma_L}$.

Definizione 2.4.24. Un Γ-modulo M è detto liscio se vale $M = \bigcup M^{\Sigma_L}$, dove l'unione è fatta sulle L finite di Galois.

Definizione 2.4.25. Possiamo definire $H^q_{cont}(\Gamma, M) = \varinjlim H^q(\Gamma_L, M^{\Sigma_L})$, dove il sistema diretto è dato dalle L estensioni finite di Galois e le mappe sono le inflazioni.

Lemma 2.4.26. *Sia $0 \to A_i \to B_i \to C_i \to 0$ una successione esatta per ogni indice i; allora vale $0 \to \varinjlim A_i \to \varinjlim B_i \to \varinjlim C_i \to 0$.*

Lemma 2.4.27. *Sia M un Γ-modulo continuo, e $M = \bigcup M_\alpha$ con α insieme filtrante. Allora $\varinjlim H^q(\Gamma, M_\alpha) = H^q_{cont}(\Gamma, M)$.*

Teorema 2.4.28. *Sia $0 \to A \to B \to C \to 0$ una successione esatta di moduli lisci. Allora ho la successione esatta lunga in coomologia con gli H^q_{cont}.*

Teorema 2.4.29. *Sia E un campo, F la sua chiusura separabile e $\Gamma = \mathrm{Gal}\left({}^{F}\!/_{E}\right)$. Allora il gruppo di Brauer di E è $\mathcal{A} = \mathcal{A}_F \cong H^2(\Gamma, F^*)$.*

2.5 Costruzione dei funtori derivati

Risoluzione iniettiva

Definizione 2.5.1. Un oggetto I è detto iniettivo se

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] \arrow[d] & Y \arrow[dl, dashed] \\ & I & \end{tikzcd}$$

Osservazione. Prodotto di iniettivi è iniettivo.

Definizione 2.5.2. Un A-modulo I è *divisibile* se $\forall x \in I, a \in A \setminus 0$ esiste un $y \in I$ tale che $ay = x$.

Teorema 2.5.3. *Se A è un PID e I è un A-modulo, allora I è iniettivo se e solo se è divisibile*

Corollario 2.5.4. *$\mathbb{Q}$ e $\mathbb{Q}/\mathbb{Z}$ sono degli $\mathbb{Z}$-moduli iniettivi.*

Proposizione 2.5.5. *Sia M uno $\mathbb{Z}$-modulo. Allora esiste un modulo iniettivo I e un'immersione $\varphi : M \to I$.*

Lemma 2.5.6. *Sia M un A-modulo e N uno $\mathbb{Z}$-modulo. Allora vale $\mathrm{Hom}_{\mathbb{Z}}(M, N) \cong \mathrm{Hom}_A(M, N_A)$, dove $N_A = \mathrm{Hom}_{\mathbb{Z}}(A, N)$ che è un A-modulo con l'azione $(a \cdot \varphi)(x) = \varphi(xa)$.*
In particolare il funtore N_A manda iniettivi in iniettivi.

Teorema 2.5.7. *Sia M un A-modulo. Allora esiste un A-modulo iniettivo I tale che $0 \to M \to I$. Ovvero Mod_A ha abbastanza iniettivi.*

Corollario 2.5.8. *Ogni A-modulo ammette una risoluzione iniettiva, costruita nel seguente modo*

$$\begin{tikzcd} & & & & {}^{I^1}\!/_{I^0} \arrow[dr] & \\ 0 \arrow[r] & M \arrow[r] & I^0 \arrow[rr] \arrow[dr] & & I^1 \arrow[r] \arrow[u] & I^2 \\ & & & {}^{I^0}\!/_{M} \arrow[ur] & & \end{tikzcd}$$

Teorema 2.5.9. *Sia $\mathcal{C}$ la categoria degli A-moduli. Sia $\mathcal{F} \subset \mathcal{C}$ una classe di moduli tali che $\forall M \in \mathcal{C}\ \exists I \in \mathcal{F}$ tale che $0 \to M \to I$.*
Allora dato un $M^\bullet \in \mathrm{Com}^+(\mathcal{C})$ esiste $X^\bullet \in \mathrm{Com}^+(\mathcal{F})$ con una mappa $\varphi : M^\bullet \to X^\bullet$ che è un quasi isomorfismo e iniettiva in ogni grado.

Categorie triangolate

Definizione 2.5.10. Sia $\mathcal{C}$ una categoria additiva con un funtore invertibile $[1]$, e una famiglia di triangoli distinti $X \to Y \to Z \to X[1]$. $\mathcal{C}$ si dice *pretriangolata* se valgono

TR1 a) $\forall X \in \mathcal{C}$ il triangolo $X = X \to 0 \to X[1]$ è distinto.
b) $\forall \varphi : X \to Y$ esiste un triangolo distinto $X \to Y \to Z \to X[1]$.
c) Un triangolo isomorfo ad un distinto è ancora distinto.

TR2 Il triangolo $X \to Y \to Z \to X[1]$ è distinto se e solo se $Y \to Z \to X[1] \to Y[1]$ è distinto.

TR3

$$\begin{tikzcd}
X \arrow[r] \arrow[d] & Y \arrow[r] \arrow[d] & Z \arrow[r] \arrow[d, dashed] & X[1] \arrow[d] \\
X' \arrow[r] & Y' \arrow[r] & Z' \arrow[r] & X'[1]
\end{tikzcd}$$

Teorema 2.5.11. *Se $\mathcal{C}$ è abeliana, la categoria $\mathrm{Kom}^+(\mathcal{C})$, con funtore $(X[1])^n = X^{n+1}$ e $\partial^n_{X[1]} = -\partial^{n+1}_X$, e triangoli distinti della forma $X \xrightarrow{\varphi} Y \to C(\varphi) \to X[1]$ dati da $C(\varphi)^n = Y^n \oplus X^{n+1}$ e $\partial^n_{C(\varphi)} = \begin{pmatrix} \partial_Y & \varphi \\ 0 & -\partial_X \end{pmatrix}$ è pretriangolata.*

Proposizione 2.5.12. *Sia $X \to Y \to Z \to X[1]$ un triangolo distinto in una categoria pretriangolata. Allora $\forall U$ la successione $\mathrm{Hom}(U, X) \to \mathrm{Hom}(U, Y) \to \mathrm{Hom}(U, Z) \to \mathrm{Hom}(U, X[1])$ è esatta di gruppi abeliani.*

Proposizione 2.5.13. *Sia $X^\bullet \to Y^\bullet \to Z^\bullet \to X^\bullet[1]$ un triangolo distinto nella categoria omotopica degli A-moduli. Allora per ogni i la successione $H^i(X) \to H^i(Y) \to H^i(Z) \to H^{i+1}(X)$ è esatta.*

Proposizione 2.5.14. *Sia $0 \to X^\bullet \xrightarrow{\varphi} Y^\bullet \xrightarrow{\pi} Z^\bullet \to 0$ una successione esatta di complessi. Consideriamo la mappa $F : C(\varphi) \to Z$ data da $F(y, x) = \pi(y)$. Questa è un quasi isomorfismo, e inoltre fa commutare il diagramma*

$$\begin{tikzcd}
H^i(X) \arrow[r] \arrow[d, equal] & H^i(Y) \arrow[r] \arrow[d, equal] & H^i(Z) \arrow[r, "-\omega"] & H^{i+1}(X) \arrow[d, equal] \\
H^i(X) \arrow[r] & H^i(Y) \arrow[r] & H^i(C(\varphi)) \arrow[r] \arrow[u, "H^i(F)"] & H^{i+1}(X)
\end{tikzcd}$$

Funtori derivati

Lemma 2.5.15. *Sia $X^\bullet$ un complesso esatto, e $I^\bullet$ un complesso di oggetti iniettivi. Allora $\mathrm{Hom}_{\mathrm{Kom}}(X, I) = 0$.*

Proposizione 2.5.16. *Siano A, B complessi e I complesso iniettivo.*

1. *Se $\varphi : A \to B$ è un quasi isomorfismo, allora* $\mathrm{Hom}_{\mathrm{Kom}}(B, I) \to \mathrm{Hom}_{\mathrm{Kom}}(A, I)$ *è un isomorfismo.*

2. *La risoluzione iniettiva di un complesso è unica in* Kom *a meno di unico isomorfismo.*

3. *Dette $A \to I_A$ e $B \to I_B$ le risoluzioni iniettive, c'è una mappa iniettiva* $\mathrm{Hom}_{\mathrm{Kom}}(A, B) \hookrightarrow \mathrm{Hom}_{\mathrm{Kom}}(I_a, I_B)$.

Definizione 2.5.17. Sia $F : \mathcal{A} \to \mathcal{B}$ un funtore additivo di categorie abeliane; supponiamo che $\mathcal{A}$ abbia abbastanza iniettivi.
Per ogni $X \in \mathrm{Com}^+(\mathcal{A})$ esiste una (unica in Kom) risoluzione iniettiva I_X.
Definiamo allora $RF : \mathrm{Kom}^+(\mathcal{A}) \to \mathrm{Kom}^+(\mathcal{B})$ tramite $RF(X) = F(I_X)$.
Sia poi $R^iF : \mathrm{Kom}^+(\mathcal{A}) \to \mathcal{B}$ dato da $R^iF(X) = H^i(RF(X))$.

Osservazione. Se F è esatto a sinistra, allora $R^0F(X) = F(X)$.

Proposizione 2.5.18. *Il funtore RF manda triangoli distinti in triangoli distinti.*

Definizione 2.5.19. Sia $\mathcal{A}$ categoria abeliana, $X \in \mathcal{A}$. Definiamo $F_X(Y) = \mathrm{Hom}(X, Y)$ e $\underline{F_X}(Y) = \mathrm{Hom}(Y, X)$.
Definiamo allora

- $\mathrm{Ext}^i(X, Y) = R^iF_X(Y)$ per $Y \in \mathrm{Com}^+(\mathcal{A})$.
- $\underline{\mathrm{Ext}^i}(X, Y) = R^i\underline{F_Y}(X)$ per $X \in \mathrm{Com}^+(\mathcal{A})$ (devo usare una risoluzione proiettiva, perché è controvariante).

Definizione 2.5.20. Un complesso doppio è un insieme di oggetti $X^{i,j}$ e mappe $\partial_O^{i,j}$ e $\partial_V^{i,j}$ messi così:

$$\begin{tikzcd}
 & {} & {} & \\
{} \arrow[r] & X^{i,j+1} \arrow[u] \arrow[r] & X^{i+1,j+1} \arrow[u] \arrow[r] & {} \\
{} \arrow[r] & X^{i,j} \arrow[u, "\partial_V^{i,j}"] \arrow[r, "\partial_O^{i,j}"] & X^{i+1,j} \arrow[u] \arrow[r] & {} \\
 & {} \arrow[u] & {} \arrow[u] &
\end{tikzcd}$$

Sia poi $T^n = \bigoplus_{i+j=n} X^{i,j}$ il complesso totale, con bordi $\partial_T^n\big|_{X^{i,j}} = \partial_O^{i,j} + (-1)^i\partial_V^{i,j}$.

Proposizione 2.5.21. *Sia $X^{i,j}$ un complesso doppio con $X^{i,j} = 0$ per $i < 0$ o $j < 0$. Supponiamo inoltre che le righe e le colonne siano esatte, tranne al più in 0; definiamo $A^j = \ker \partial_O^{0,j}$ e $B^i = \ker \partial_V^{i,0}$. Siano poi $\alpha : A^\bullet \to T$ e $\beta : B^\bullet \to T$ le inclusioni.*
Allora α, β sono mappe di complessi e quasi isomorfismi.

Proposizione 2.5.22. *Siano X, Y oggetti. Allora* $\mathrm{Ext}^i(X, Y) = \underline{\mathrm{Ext}^i}(X, Y)$