

Appunti del corso  
Istituzioni di algebra

Riccardo Zanotto, Andrea Gallese

25 settembre 2019

---

# Indice

<b>Indice</b>	<b>ii</b>
<b>1 Algebra commutativa</b>	<b>1</b>
1.1 Estensioni intere . . . . .	1
1.2 Dimensione . . . . .	3
1.3 Azione di Galois . . . . .	4
1.4 Valutazioni e completamenti . . . . .	5
<b>2 Algebra omologica</b>	<b>6</b>
2.1 $E$ -strutture e $H^1$ di gruppi . . . . .	6
2.2 Categorie, categorie abeliane e complessi . . . . .	7
2.3 Coomologia di gruppi . . . . .	10
2.4 Gruppo di Brauer . . . . .	11
2.5 Costruzione dei funtori derivati . . . . .	14

# Algebra commutativa

**Lemma 1.** Sia  $\varphi : A \rightarrow B$  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 2.** Sia  $A$  un PID: un modulo  $M$  è piatto se e solo è libero da torsione.

## 1.1 Estensioni intere

**Definizione.** 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  $f : A \rightarrow B$  è morfismo di anelli con 1,  $I \subset A$ , diciamo che  $b$  è intero su  $I$  se lo è su  $I^e$ .

**Proposizione 3** (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.** 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 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 5.** Sia  $A \subset B$  intera,  $I \subset A$  ideale. Detto  $\bar{I}^B = \{b \in B \mid b \text{ è intero su } I\}$ , vale  $\bar{I}^B = \sqrt{I^e}$ .

**Proposizione 6.** Sia  $A \subset B$  intera,  $J$  ideale di  $B$ ,  $S$  parte moltiplicativa di  $A$ . Abbiamo che:

- $A/J^e \subset B/J$  è intera;
- $\overline{S^{-1}A}^{S^{-1}B} = S^{-1}(\bar{A}^B)$ .

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

**Proposizione 7.** Ogni UFD è normale.

**Teorema 8 (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  $x \in \bar{I}^L \iff \mu_x(t) \in \sqrt{I}[t]$ . In particolare

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

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

**Lemma 9.** Sia  $A \subset B$  intera di domini. Allora  $A$  è un campo se e solo se  $B$  è un campo.

**Corollario 10.** Sia  $A \subset B$  intera,  $\mathfrak{p} \subset B$  primo. Allora  $\mathfrak{p}$  è massimale se e solo se  $\mathfrak{p}^e$  è massimale.

**Corollario 11.** Sia  $A \subset B$  intera,  $\mathfrak{p} \subset \mathfrak{q} \subset B$  ideali primi. Se  $\mathfrak{p}^e = \mathfrak{q}^e$  allora  $\mathfrak{p} = \mathfrak{q}$ .

**Teorema 12 (Lying over).** Sia  $A \subset B$  intera. Allora  $\varphi : \text{Spec } B \rightarrow \text{Spec } A$  è surgettiva.

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

**Teorema 13 (Going Down).** Sia  $A \subset B$ .

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

**Proposizione 14.** Sia  $A \subset B$ ; se vale il going up e  $B$  è noetheriano, allora  $\varphi : \text{Spec } B \rightarrow \text{Spec } A$  è chiusa.

**Lemma 15** (degli Aperti). Sia  $f : A \rightarrow B$ , e  $\varphi : Y = \text{Spec } B \rightarrow \text{Spec } A = X$ ; dato  $\mathfrak{q} \in Y$ , definiamo  $Y_{\mathfrak{q}} = \text{Spec } B_{\mathfrak{q}} = \{r \in Y \mid r \subset \mathfrak{q}\}$ . Allora

1.  $Y_{\mathfrak{q}} = \bigcap_{\alpha \not\subset \mathfrak{q}} Y_{\alpha}$
2.  $\varphi(Y_{\mathfrak{q}}) = \bigcap_{\alpha \not\subset \mathfrak{q}} \varphi(Y_{\alpha})$

**Teorema 16** (Going Down). Sia  $f : A \rightarrow B$  e  $\varphi : \text{Spec } B \rightarrow \text{Spec } A$ . Se  $\varphi$  è aperta, allora vale il going down per  $f$ .

**Teorema 17.** Sia  $A \subset B$  intera con  $A, B$  domini, e  $A$  normale. Allora  $\varphi : \text{Spec } B \rightarrow \text{Spec } A$  è aperta.

**Proposizione 18.** Sia  $f : A \rightarrow B$ , e supponiamo che valga il going down; se  $A$  è noetheriano, allora  $\varphi$  è aperta.

## 1.2 Dimensione

**Definizione.** 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 19.** Se  $A \subset B$  è intera, allora  $\dim A = \dim B$ .

**Teorema 20.** 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 21.** 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.** 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 22.** Se  $x_{\alpha}$  è base di trascendenza di  $A$  su  $k$ , allora l'estensione  $k(x_{\alpha}) \subset \mathbb{Q}(A)$  è algebrica.

**Teorema 23.** Tutte le basi di trascendenza hanno la stessa cardinalità.

**Corollario 24.** Se  $A$  è una  $k$ -algebra fin. gen. e un dominio, allora  $\dim A = \text{Tr deg}_k A$ .

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

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

**Lemma 25.** 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 26.** Sia  $A$  una  $k$ -algebra fin. gen. Allora

1. Se  $\mathfrak{p} \in \text{Spec } A$ , allora  $\text{ht}(\mathfrak{p}), \text{coht}(\mathfrak{p}) < \infty$ .
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  $\text{coht}(\mathfrak{p}) - \text{coht}(\mathfrak{q})$ .
3. Se  $A$  è un dominio,  $\mathfrak{p} \in \text{Spec } A$ , allora vale  $\dim A = \text{ht}(\mathfrak{p}) + \text{coht}(\mathfrak{p})$ .

Cosa succede in dimensione bassa?

**Teorema 27.** *Sia  $A$  un anello. Allora  $A$  è artiniano se e solo se è noetheriano e  $\dim A = 0$ .*

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

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

**Proposizione 28.** *Se esiste una catena di sottomoduli massimale di lunghezza finita, allora sono tutte finite e della stessa lunghezza.*

**Proposizione 29.** *La lunghezza  $l(M)$  è finita se e solo se  $M$  è artiniano e noetheriano.*

**Teorema 30.** *Se  $A \subseteq B$  è finita, si trovano solo finiti primi di  $Q$  sopra ogni  $\mathfrak{p} \in \text{Spec } A$ .*

### 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  $B = \overline{A}^L$ :

$$\begin{array}{ccc} B & \text{---} & L \\ | & & | \\ A & \text{---} & K. \end{array}$$

Definiamo  $Y = \text{Spec } B$ ,  $X = \text{Spec } A$ ,  $\varphi: Y \rightarrow X$ ; 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 31.** *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 32.** *Il gruppo  $G$  agisce transitivamente sull'insieme  $Y_{\mathfrak{p}}$ .*

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

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

**Proposizione 33.**  *$G_{\mathfrak{q}}$  agisce dunque su  $k(\mathfrak{q})$  tenendo fisso  $k(\mathfrak{p})$ , e la mappa*

$$G_{\mathfrak{q}} \rightarrow \{\varphi: k(\mathfrak{q}) \rightarrow k(\mathfrak{q}) \mid \varphi|_{k(\mathfrak{p})} = \text{id}\} = \text{Gal}\left(k(\mathfrak{q}) / k(\mathfrak{p})\right)$$

*è surgettiva.*

**Teorema 34.** *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 35** (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.** Sia  $k$  un campo; una mappa  $v : k^* \rightarrow \mathbb{Q}$  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  $\text{Im } v = \mathbb{Z} \cdot q$  per qualche  $q \neq 0$ ; in questo caso  $A$  è un DVR.

**Proposizione 36.** *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  $(\pi^m)$  dove  $v(\pi) = q$ .*

**Teorema 37.** *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 valgono le condizioni sopra, allora  $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$ .

**Proposizione 38.** *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  $f = 0$ .*

## Algebra omologica

### 2.1 $E$ -strutture e $H^1$ di gruppi

**Lemma 39.** *Sia  $E \subset F$  finita di Galois con gruppo  $\Gamma$ ;  $V$  un  $E$ -spazio vettoriale.*

1. *Detto  $V_F = F \otimes_E V$ ,  $\Gamma$  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  $\Gamma$  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  $F \otimes_E W_0 \rightarrow W$  che manda  $\lambda \otimes v \mapsto \lambda v$  è un isomorfismo

**Teorema 40.** *Sia  $E \subset F$  un'estensione di Galois infinita. Allora*

$$\text{Gal}\left(\frac{F}{E}\right) \cong \varprojlim_{[L:E] < \infty} \text{Gal}\left(\frac{L}{E}\right)$$

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

**Lemma 41.** *Sia  $E \subset F$  di Galois infinita,  $V$  un  $F$ -spazio vettoriale; supponiamo che  $\Gamma = \text{Gal}\left(\frac{F}{E}\right)$  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.** Sia  $E \subset F$  estensione di Galois con gruppo  $\Gamma$ ; siano  $A_0, B$  due  $E$ -algebre, e  $R = F \otimes A_0 \cong F \otimes B$ . Sia  $\gamma_0 = \gamma \otimes_E \text{id}_{A_0}$  l'azione di  $\Gamma$  estesa su  $R$ , e similmente  $\gamma_B$ .

Sia  $c : \Gamma \rightarrow \text{Aut}(R)$  dato da  $c_\gamma = \gamma_B \cdot \gamma_A^{-1}$ .

**Proposizione 42.**

- Per ogni  $\gamma$ ,  $c_\gamma$  è  $F$ -lineare, quindi ho definito  $c : \Gamma \rightarrow \text{Aut}_F(R)$
- Vale  $c_{\gamma\delta} = c_\gamma \circ^\gamma c_\delta$ , dove  ${}^\gamma\varphi = \gamma_0 \circ \varphi \circ \gamma_0^{-1}$



**Definizione.** Definiamo  $Z^1(\Gamma, \text{Aut}_F(R)) = \{c : \Gamma \rightarrow \text{Aut}_F(R) \mid c_{\gamma\delta} = c_\gamma \circ^\gamma c_\delta\}$ .

Se  $c, c' \in Z^1$ , diciamo che  $c \sim c'$  se  $\exists f \in \text{Aut}_F R$  tale che  $c'_\gamma = f \circ c_\gamma \circ^\gamma f^{-1}$ .

Definiamo poi  $H^1(\Gamma, \text{Aut}_F(R)) = Z^1(\Gamma, \text{Aut}_F(R)) / \sim$

**Teorema 43.**

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

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

**Definizione.** Sia  $Z^1(\Gamma, G) = \{c : \Gamma \rightarrow G \mid c_{\gamma\delta} = c_\gamma \cdot^\gamma c_\delta\}$ .

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 44.** Sia  $1 \rightarrow H \rightarrow G \rightarrow K \rightarrow 1$  una successione esatta di gruppi su cui agisce  $\Gamma$  in modo compatibile con le mappe.

Allora  $1 \rightarrow H^\Gamma \rightarrow G^\Gamma \rightarrow K^\Gamma \rightarrow H^1(\Gamma, H) \rightarrow H^1(\Gamma, G) \rightarrow H^1(\Gamma, K)$  è una successione esatta di insiemi puntati.

**Teorema 45** (Hilbert 90). Sia  $E \subset F$  di Galois finita con gruppo  $\Gamma$ ; sia  $G = \text{GL}_n(F)$  e  $\Gamma$  agisce su  $G$  coefficiente per coefficiente. Allora  $H^1(\Gamma, \text{GL}_n(F)) = \{1\}$ .

**Corollario 46.** Anche  $H^1(\Gamma, \text{SL}_n(F)) = \{1\}$ .

**Proposizione 47.** Sia  $x_0 \in X^\Gamma$  e  $H = \text{stab}_G x_0$ ; supponiamo che  $G$  agisca transitivamente su  $X$ . Se  $H^1(\Gamma, G) = \{1\}$ , allora le orbite di  $G^\Gamma$  in  $X^\Gamma$  sono in bigezione con  $H^1(\Gamma, H)$ .

## 2.2 Categorie, categorie abeliane e complessi

**Lemma 48** (di Yoneda). Sia  $\mathcal{C}$  una categoria piccola e  $F: \mathcal{C} \rightarrow \mathbf{Set}$  un funtore controvariante nella categoria degli insiemi. Si ha una bigezione

$$\text{Nat}(h_X, F) \leftrightarrow F(X).$$

**Proposizione 49** (che fa impallidire anche Yoneda). I limiti sono coequalizzatori. Sia  $I$  un sistema proiettivo, allora  $\varprojlim F(i)$  è isomorfo all'equalizzatore del diagramma

$$\prod_i F(i) \xrightleftharpoons[S]{T} \prod_{\varphi: i \rightarrow j} F(j)_\varphi$$

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

$$\begin{array}{ccc} \prod_i F(i) & \xrightarrow{T} & \prod_{\varphi: i \rightarrow j} F(j)_\varphi \\ \downarrow \pi_b & & \downarrow \pi_{b\varphi} \\ F(b) & \xrightarrow{\text{id}} & F(b)_\varphi \end{array} \qquad \begin{array}{ccc} \prod_i F(i) & \xrightarrow{S} & \prod_{\varphi: i \rightarrow j} F(j)_\varphi \\ \downarrow \pi_a & & \downarrow \pi_{b\varphi} \\ F(a) & \xrightarrow{\varphi} & F(b)_\varphi \end{array}$$

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

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

$$\begin{array}{ccccc} & & Z & & \\ & f \nearrow & \uparrow & \nwarrow g & \\ X & \xrightarrow{i_X} & X \amalg Y & \xleftarrow{i_Y} & Y \end{array}$$

**Proposizione 50.** In una categoria additiva, il coprodotto è isomorfo al prodotto, e si indica con  $X \oplus Y$ .

**Definizione.** Fissata una mappa  $\varphi : X \rightarrow Y$ , diciamo che:

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

$$\begin{array}{ccc} Z & \xrightarrow{\ell} & X \xrightarrow{\varphi} Y \\ & \nwarrow \tilde{\alpha} & \uparrow \alpha \\ & & U \end{array}$$

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

$$\begin{array}{ccccc} X & \xrightarrow{\varphi} & Y & \xrightarrow{m} & Q \\ & & \downarrow \beta & \nwarrow \tilde{\beta} & \\ & & U & & \end{array}$$

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

$$\begin{array}{ccccccc} K & \xrightarrow{\alpha} & X & \xrightarrow{\varphi} & Y & \xrightarrow{\beta} & Q \\ & & \downarrow \pi & \nearrow \psi & \uparrow j & & \\ & & \text{coker } \alpha & \xrightarrow[\cong]{\sim} & \ker \beta & & \end{array}$$

**Proposizione 51.** In una categoria abeliana  $\varphi$  è un isomorfismo se e solo se  $\ker \varphi = 0$  e  $\text{coker } \varphi = 0$ .

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

**Proposizione 52.** In una categoria abeliana valgono lo snake lemma e il lemma dei 5.

**Lemma 53.** Nella categoria degli  $A$ -moduli il limite inverso  $\varprojlim$  è esatto a sinistra.

**Teorema 54.** In realtà le categorie abeliane sono gli  $A$ -moduli...

## Complessi

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

**Definizione.** 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*  $\varphi^\bullet : X^\bullet \rightarrow Y^\bullet$  è una successione di mappe  $\varphi^n : X^n \rightarrow Y^n$  tali che tutti i quadrati commutino:

$$\begin{array}{ccccc} X^{n-1} & \xrightarrow{\partial_X^{n-1}} & X^n & \xrightarrow{\partial_X^n} & X^{n+1} \\ \downarrow \varphi^{n-1} & & \downarrow \varphi^n & & \downarrow \varphi^{n+1} \\ Y^{n-1} & \xrightarrow{\partial_Y^{n-1}} & Y^n & \xrightarrow{\partial_Y^n} & Y^{n+1} \end{array}$$

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

**Proposizione 55.** *Le categorie  $\text{Com}(\mathcal{C})$ ,  $\text{Com}^+(\mathcal{C})$  e  $\text{Com}^-(\mathcal{C})$  sono abeliane.*

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

**Proposizione 56.** *Se  $\varphi^\bullet : X^\bullet \rightarrow Y^\bullet$  è morfismo di complessi, otteniamo una successione di mappe  $H^n(\varphi) : H^n(X) \rightarrow H^n(Y)$ .*

**Teorema 57.** *Sia  $0 \rightarrow X^\bullet \xrightarrow{\varphi^\bullet} Y^\bullet \xrightarrow{\psi^\bullet} Z^\bullet \rightarrow 0$  una successione esatta di complessi. Allora la successione*

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

*è esatta.*

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

**Proposizione 58.** *Se  $\varphi \sim 0$ , allora vale  $H^n(\varphi) = 0$ ; in particolare se vale  $\text{id} \sim 0$ , allora il complesso è esatto.*

**Definizione.** 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  $\varphi^\bullet : X^\bullet \rightarrow Y^\bullet$  che sia un isomorfismo in coomologia.

**Definizione.** Sia  $A \in \mathcal{C}$  e  $F : \mathcal{C} \rightarrow \mathcal{C}'$  un funtore additivo, esatto a sinistra.

Sia  $I^\bullet$  una risoluzione iniettiva del complesso  $\dots \rightarrow 0 \rightarrow A \rightarrow 0 \rightarrow \dots$ .

Definiamo l' $i$ -esimo funtore derivato come  $R^i F(A) = H^i(FI^\bullet)$  l' $i$ -esimo gruppo di coomologia del complesso  $0 \rightarrow FI^0 \rightarrow FI^1 \rightarrow \dots$ .

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

**Definizione.** 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 proiettivi ed esiste un morfismo di complessi  $\varphi^\bullet : P^\bullet \rightarrow X^\bullet$  che sia un isomorfismo in coomologia.

**Definizione.** Sia  $A \in \mathcal{C}$  e  $F : \mathcal{C} \rightarrow \mathcal{C}'$  un funtore controvariante, additivo, esatto a sinistra.

Sia  $P^\bullet$  una risoluzione iniettiva del complesso  $\dots \rightarrow 0 \rightarrow A \rightarrow 0 \rightarrow \dots$ .

Definiamo l' $i$ -esimo funtore derivato come  $L^i F(A) = H^i(FP^\bullet)$  l' $i$ -esimo gruppo di coomologia del complesso  $0 \rightarrow FP^0 \rightarrow FP^1 \rightarrow \dots$ .

**Definizione.** Siano  $X, Y$  oggetti; siano  $F, G$  i funtori  $F = \text{Hom}(X, -)$  e  $G = \text{Hom}(-, Y)$ .

Definiamo allora  $\text{Ext}^i(X, Y) = R^i F(Y)$  e  $\underline{\text{Ext}}^i(X, Y) = L^i G(X)$ .

**Esempio.** Siano  $m, n \in \mathbb{Z}$  e scriviamo  $m = dm', n = dn'$  con  $d = \text{gcd}(m, n)$ .

Allora  $\underline{\text{Ext}}^0(\mathbb{Z}/(m), \mathbb{Z}/(n)) \cong \underline{\text{Ext}}^1(\mathbb{Z}/(m), \mathbb{Z}/(n)) \cong \mathbb{Z}/(d)$ .

**Proposizione 59.** Se  $X, Y$  sono oggetti, allora  $\text{Ext}^i(X, Y) \cong \underline{\text{Ext}}^i(X, Y)$ .

## 2.3 Coomologia di gruppi

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

**Definizione.** Sia  $M$  un  $R[G]$ -modulo; definiamo  $F_1(M) = M^G = \text{Hom}_{R[G]}(R, M)$

e  $F_2(M) = M / \langle m - gm \rangle = R \otimes_{R[G]} M$ .

Definiamo  $H^n(G, M) = \text{Ext}^n(R, M) = R^n F_1(M)$ ; sappiamo però che è isomorfo a  $\underline{\text{Ext}}^n(R, M)$ , che è il funtore derivato di  $\text{Hom}_{R[G]}(-, M)$ .

Inoltre  $H_n(G, M) = \text{Tor}_n(R, M)$  il funtore derivato di  $F_2$ .

**Proposizione 60** (risoluzione libera di  $R$ ). Siano  $P^0 = R[G], P^{-1} = R[G \times G], P^{-2} = R[G \times G \times G], \dots$ ; sia  $\varepsilon : P^0 \rightarrow R$  data da  $\varepsilon(g) = 1$ .

Sia poi  $\partial^{-n} : P^{-n} \rightarrow P^{-n+1}$  data da

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

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

**Proposizione 61.** La mappa  $\Phi_n : \text{Hom}_{R[G]}(P^{-n}, M) \rightarrow \{f : G^n \rightarrow M\} =: C^n(G, M)$  data da  $\Phi_n(\psi)(g_1, \dots, g_n) = \psi(1, g_1, g_1 g_2, \dots, g_1 \cdots g_n)$  è un isomorfismo.

Inoltre la mappa  $\delta_C^n : C^n(G, M) \rightarrow C^{n+1}(G, M)$  data da  $\delta_C^n f = \Phi_{n+1}((\Phi_n^{-1} f) \circ \partial^{-n})$  ha la formula esplicita

$$\begin{aligned} (\delta_C^n f)(g_1, \dots, g_{n+1}) &= g_1 \cdot f(g_2, \dots, g_{n+1}) + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i \cdot g_{i+1}, \dots, g_{n+1}) \\ &\quad + (-1)^n f(g_1, \dots, g_n) \end{aligned}$$

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

**Definizione.** Sia  $f : H \rightarrow G$  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  $C^q(G, M) \rightarrow C^q(H, M)$ , da cui si ottiene una mappa  $\text{Res}^q : H^q(G, M) \rightarrow H^q(H, f^*M)$  in coomologia.

**Definizione.** Sia  $f : H \rightarrow G$  un omomorfismo di gruppi e  $N$  un  $H$ -modulo. Definiamo  $\text{Ind}_H^G N = R[G] \otimes_{R[H]} N$  che è un  $G$ -modulo tramite  $g \cdot (x \otimes n) = xg \otimes n$ . Definiamo poi  $\text{coInd}_H^G N = \text{Hom}_H(R[G], N)$ , 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 62.** Sia  $M$  un  $G$ -modulo e  $N$  un  $H$ -modulo, e  $f : H \rightarrow G$ . Allora valgono

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

**Proposizione 63.** Siano  $F, G$  due funtori aggiunti tra due categorie  $\mathcal{A}, \mathcal{B}$ , ovvero tali che  $\text{Hom}_{\mathcal{A}}(a, Gb) = \text{Hom}_{\mathcal{B}}(Fa, b)$ . 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 64.** Sia  $H < G$  e  $N$  un  $H$ -modulo. Allora

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

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

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

Inoltre, se  $0 \rightarrow M \rightarrow I_M^\bullet$  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:

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

**Proposizione 65.** Sia  $H < G$  di indice finito. Allora  $\text{coRes}^q \circ \text{Res}^q = [G : H] \text{id}$ .

**Corollario 66.** 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.** 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 67.** 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.** Un anello  $A$  si dice semisemplice se lo è come  $A$ -modulo sinistro.

**Proposizione 68.** Sia  $A$  un anello. Sono equivalenti

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

**Lemma 69** (Schur). Siano  $S, T$  moduli semplici. Allora

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

**Teorema 70** (Wedderburn). Sia  $A$  un anello semisemplice. Allora  $A = \bigoplus_i \text{Mat}_{n_i \times n_i}(D_i)$  con  $D_i$  corpi univocamente determinati.

**Proposizione 71.** Sia  $E = \overline{E}$ , e  $D \supset E$  un corpo di dimensione finita con  $E \subset Z(D)$ . Allora  $D = E$ .

**Definizione.** 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 72.** Sia  $A$  una  $E$ -algebra di dimensione finita. Sono equivalenti

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

**Corollario 73.**  $A$  è un' $E$ -algebra centrale semplice se e solo se  $A = \text{Mat}_{n \times n}(D)$ , con  $Z(D) = E$ .

**Lemma 74.** 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 75.** Sia  $A$  una  $E$ -acs;  $E \subset F$  estensione di campi. Allora  $F \otimes_E A$  è una  $F$ -acs.

**Teorema 76.** Siano  $A, A'$  delle  $E$ -acs. Allora anche  $A \otimes_E A'$  è una  $E$ -acs.

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

**Teorema 77.** *Sia  $A$  una  $E$ -acs. Allora esiste un'estensione di campi  $E \subset F$  finita e separabile tale che  $A$  spezza su  $F$ .*

**Definizione.** Sia  $E$  un campo; definiamo il suo gruppo di Brauer come  $\mathcal{A} = \{E\text{-acs}\}/\sim$ , 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  $A \otimes A^{op} = \text{End}_E(A) = \text{Mat}_{n \times n}(E)$ .

### Descrizione coomologica

**Lemma 78.** *Dato un campo  $F$  vale  $\text{Aut}_F(\text{Mat}_{n \times n}(F)) = \text{PGL}_n(F)$*

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

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

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

**Definizione.** Definiamo la mappa  $\delta_{n,L} : \mathcal{A}_{n,L} \rightarrow H^2(\Gamma, L^*)$  tramite la successione lunga data da  $1 \rightarrow L^* \rightarrow \text{GL}_n(L) \rightarrow \text{PGL}_n(L) \rightarrow 1$ .

**Lemma 79.** *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  $\delta_k$  è surgettiva per  $k = [L : E]$ .

**Teorema 80.** *Le mappe  $\delta_n$  permettono di costruire l'isomorfismo di gruppi*

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

**Corollario 81.**

- 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.** In generale, sia  $G$  un gruppo,  $H \trianglelefteq G$  e  $M$  un  $G$ -modulo. La mappa naturale  $\text{Inf}^q : H^q(G/H, M^H) \rightarrow H^q(G, M)$  è detta *inflazione*.

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

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

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

**Lemma 82.** Sia  $0 \rightarrow A_i \rightarrow B_i \rightarrow C_i \rightarrow 0$  una successione esatta per ogni indice  $i$ ; allora vale  $0 \rightarrow \varinjlim A_i \rightarrow \varinjlim B_i \rightarrow \varinjlim C_i \rightarrow 0$ .

**Lemma 83.** Sia  $M$  un  $\Gamma$ -modulo continuo, e  $M = \bigcup M_\alpha$  con  $\alpha$  insieme filtrante. Allora  $\varinjlim H^q(\Gamma, M_\alpha) = H_{cont}^q(\Gamma, M)$ .

**Teorema 84.** Sia  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  una successione esatta di moduli lisci. Allora ho la successione esatta lunga in coomologia con gli  $H_{cont}^q$ .

**Teorema 85.** Sia  $E$  un campo,  $F$  la sua chiusura separabile e  $\Gamma = \text{Gal}(F/E)$ . 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.** Un oggetto  $I$  è detto iniettivo se

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \longrightarrow & Y \\ & & \downarrow & \swarrow & \\ & & I & & \end{array}$$

*Osservazione.* Prodotto di iniettivi è iniettivo.

**Definizione.** 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 86.** Se  $A$  è un PID e  $I$  è un  $A$ -modulo, allora  $I$  è iniettivo se e solo se è divisibile

**Corollario 87.**  $\mathbb{Q}$  e  $\mathbb{Q}/\mathbb{Z}$  sono degli  $\mathbb{Z}$ -moduli iniettivi.

**Proposizione 88.** Sia  $M$  uno  $\mathbb{Z}$ -modulo. Allora esiste un modulo iniettivo  $I$  e un'immersione  $\varphi : M \rightarrow I$ .

**Lemma 89.** Sia  $M$  un  $A$ -modulo e  $N$  uno  $\mathbb{Z}$ -modulo. Allora vale  $\text{Hom}_{\mathbb{Z}}(M, N) \cong \text{Hom}_A(M, N_A)$ , dove  $N_A = \text{Hom}_{\mathbb{Z}}(A, N)$  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 90.** Sia  $M$  un  $A$ -modulo. Allora esiste un  $A$ -modulo iniettivo  $I$  tale che  $0 \rightarrow M \rightarrow I$ . Ovvero  $\text{Mod}_A$  ha abbastanza iniettivi.

**Corollario 91.** Ogni  $A$ -modulo ammette una risoluzione iniettiva, costruita nel seguente modo

$$\begin{array}{ccccccc} & & & & I^1/I^0 & & \\ & & & & \nearrow & \searrow & \\ 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 \\ & & & & \searrow & \nearrow & & & \\ & & & & I^0/M & & & & \end{array}$$



**Teorema 92.** 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  $0 \rightarrow M \rightarrow I$ . Allora dato un  $M^\bullet \in \text{Com}^+(\mathcal{C})$  esiste  $X^\bullet \in \text{Com}^+(\mathcal{F})$  con una mappa  $\varphi : M^\bullet \rightarrow X^\bullet$  che è un quasi isomorfismo e iniettiva in ogni grado.

### Categorie triangolate

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

- TR1 a)  $\forall X \in \mathcal{C}$  il triangolo  $X = X \rightarrow 0 \rightarrow X[1]$  è distinto.  
 b)  $\forall \varphi : X \rightarrow Y$  esiste un triangolo distinto  $X \rightarrow Y \rightarrow Z \rightarrow X[1]$ .  
 c) Un triangolo isomorfo ad un distinto è ancora distinto.
- TR2 Il triangolo  $X \rightarrow Y \rightarrow Z \rightarrow X[1]$  è distinto se e solo se  $Y \rightarrow Z \rightarrow X[1] \rightarrow Y[1]$  è distinto.

TR3

$$\begin{array}{ccccccc} X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & X[1] \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & X'[1] \end{array}$$

**Teorema 93.** Se  $\mathcal{C}$  è abeliana, la categoria  $\text{Kom}^+(\mathcal{C})$ , con funtore  $(X[1])^n = X^{n+1}$  e  $\partial_{X[1]}^n = -\partial_X^{n+1}$ , e triangoli distinti della forma  $X \xrightarrow{\varphi} Y \rightarrow C(\varphi) \rightarrow X[1]$  dati da  $C(\varphi)^n = Y^n \oplus X^{n+1}$  e  $\partial_{C(\varphi)}^n = \begin{pmatrix} \partial_Y & \varphi \\ 0 & -\partial_X \end{pmatrix}$  è pretriangolata.

**Proposizione 94.** Sia  $X \rightarrow Y \rightarrow Z \rightarrow X[1]$  un triangolo distinto in una categoria pretriangolata. Allora  $\forall U$  la successione  $\text{Hom}(U, X) \rightarrow \text{Hom}(U, Y) \rightarrow \text{Hom}(U, Z) \rightarrow \text{Hom}(U, X[1])$  è esatta di gruppi abeliani.

**Proposizione 95.** Sia  $X^\bullet \rightarrow Y^\bullet \rightarrow Z^\bullet \rightarrow X^\bullet[1]$  un triangolo distinto nella categoria omotopica degli  $A$ -moduli. Allora per ogni  $i$  la successione  $H^i(X) \rightarrow H^i(Y) \rightarrow H^i(Z) \rightarrow H^{i+1}(X)$  è esatta.

**Proposizione 96.** Sia  $0 \rightarrow X^\bullet \xrightarrow{\varphi} Y^\bullet \xrightarrow{\pi} Z^\bullet \rightarrow 0$  una successione esatta di complessi. Consideriamo la mappa  $F : C(\varphi) \rightarrow Z$  data da  $F(y, x) = \pi(y)$ . Questa è un quasi isomorfismo, e inoltre fa commutare il diagramma

$$\begin{array}{ccccccc} H^i(X) & \longrightarrow & H^i(Y) & \longrightarrow & H^i(Z) & \xrightarrow{-\omega} & H^{i+1}(X) \\ \parallel & & \parallel & & \uparrow H^i(F) & & \parallel \\ H^i(X) & \longrightarrow & H^i(Y) & \longrightarrow & H^i(C(\varphi)) & \longrightarrow & H^{i+1}(X) \end{array}$$

### Funtori derivati

**Lemma 97.** Sia  $X^\bullet$  un complesso esatto, e  $I^\bullet$  un complesso di oggetti iniettivi. Allora  $\text{Hom}_{\text{Kom}}(X, I) = 0$ .

**Proposizione 98.** Siano  $A, B$  complessi e  $I$  complesso iniettivo.

1. Se  $\varphi : A \rightarrow B$  è un quasi isomorfismo, allora  $\text{Hom}_{\text{Kom}}(B, I) \rightarrow \text{Hom}_{\text{Kom}}(A, I)$  è un isomorfismo.
2. La risoluzione iniettiva di un complesso è unica in  $\text{Kom}$  a meno di unico isomorfismo.
3. Dette  $A \rightarrow I_A$  e  $B \rightarrow I_B$  le risoluzioni iniettive, c'è una mappa iniettiva  $\text{Hom}_{\text{Kom}}(A, B) \hookrightarrow \text{Hom}_{\text{Kom}}(I_A, I_B)$ .

**Definizione.** Sia  $F : \mathcal{A} \rightarrow \mathcal{B}$  un funtore additivo di categorie abeliane; supponiamo che  $\mathcal{A}$  abbia abbastanza iniettivi.

Per ogni  $X \in \text{Com}^+(\mathcal{A})$  esiste una (unica in  $\text{Kom}$ ) risoluzione iniettiva  $I_X$ .

Definiamo allora  $RF : \text{Kom}^+(\mathcal{A}) \rightarrow \text{Kom}^+(\mathcal{B})$  tramite  $RF(X) = F(I_X)$ .

Sia poi  $R^i F : \text{Kom}^+(\mathcal{A}) \rightarrow \mathcal{B}$  dato da  $R^i F(X) = H^i(RF(X))$ .

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

**Proposizione 99.** Il funtore  $RF$  manda triangoli distinti in triangoli distinti.

**Definizione.** Sia  $\mathcal{A}$  categoria abeliana,  $X \in \mathcal{A}$ . Definiamo  $F_X(Y) = \text{Hom}(X, Y)$  e  $\underline{F}_X(Y) = \text{Hom}(Y, X)$ .

Definiamo allora

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

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

$$\begin{array}{ccccccc}
 & & \uparrow & & \uparrow & & \\
 & & X^{i,j+1} & \longrightarrow & X^{i+1,j+1} & \longrightarrow & \\
 & \partial_V^{i,j} \uparrow & & & \uparrow & & \\
 \longrightarrow & X^{i,j} & \xrightarrow{\partial_O^{i,j}} & X^{i+1,j} & \longrightarrow & & \\
 & \uparrow & & \uparrow & & & 
 \end{array}$$

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

**Proposizione 100.** 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  $\alpha : A^\bullet \rightarrow T$  e  $\beta : B^\bullet \rightarrow T$  le inclusioni.

Allora  $\alpha, \beta$  sono mappe di complessi e quasi isomorfismi.

**Proposizione 101.** Siano  $X, Y$  oggetti. Allora  $\text{Ext}^i(X, Y) = \underline{\text{Ext}}^i(X, Y)$