ESTENSIONI E COOMOLOGIA DI GRUPPI

LUIGI CAPUTI

Un classico problema in teoria dei gruppi è quello di classificare tutte le possibili estensioni di un dato gruppo G, a meno di opportune equivalenze.

Mostreremo come questo problema di classificazione sia strettamente legato alla struttura dei gruppi di coomologia di G; in particolare concentreremo l'attenzione ai casi $\mathrm{H}^1(G)$ e $\mathrm{H}^2(G)$, per definire i quali abbiamo bisogno dei concetti di risoluzioni e G-moduli. Cominciamo dunque con il richiamare queste definizioni.

1. Risoluzioni

Sia R un anello con identità $1_R \neq 0$ ed M un *R-modulo sinistro*, ovvero un gruppo abeliano su cui R agisce linearmente a sinistra.

Definizione 1. Una *risoluzione di M* è una sequenza esatta di R-moduli

$$\dots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Diciamo inoltre che la risoluzione è *libera* se tutti gli F_i sono liberi.

Osservazione 2. Se M è un R-modulo, allora M ammette sempre una risoluzione libera. Infatti basta considerare la mappa surgettiva $\varepsilon\colon F_0 \to M$ con F_0 modulo libero e $\partial_1\colon F_1 \to \ker(\varepsilon)$ surgettiva, con F_1 modulo libero. A questo punto è possibile iterare il procedimento ottenendo la risoluzione cercata. Osserviamo che, in particolare, il primo pezzo della risoluzione è proprio la presentazione libera di M.

In quanto successione esatta, possiamo interpretare una risoluzione libera in termini di complessi di catene ad omologia nulla. Parleremo in tal caso di *complesso di catene aumentato*. Possiamo tuttavia considerare il solo complesso $\{F_i\}_{i\in\mathbb{N}}$ e vedere che, come complesso di catene, esso ammette omologia a livello 0 pari ad M. La mappa $\varepsilon\colon F_0 \to M$ è detta *mappa di aumentazione*, in analogia con il caso topologico.

Definizione 3. Se esiste un n per cui $F_i = 0\ \forall i > n$ diciamo che la risoluzione ha *lunghezza* $\leq n$, e quindi possiamo scrivere

$$0 \longrightarrow F_n \xrightarrow{\partial_n} \dots \xrightarrow{\partial_1} F_0 \xrightarrow{\epsilon} M \longrightarrow 0.$$

Esempio. (1) Se F è un modulo libero, allora

$$0 \to F \to F \to 0$$

è una risoluzione libera di lunghezza nulla.

(2) Se R è un PID, ogni sottomodulo di un R-modulo libero è libero, quindi una risoluzione libera per l'R-modulo M è data proprio dalla sua presentazione. Ad esempio

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}_n \longrightarrow 0.$$

è una risoluzione libera di $\mathbb{Z}_n$.

Abbiamo notato che ogni R-modulo M ammette una risoluzione libera, ed è anche chiaro che tale risoluzione può non essere unica. A questo scopo, ricordiamo che se (C,d) e (C',d') sono due complessi di catene, una *mappa di catene* da C in C' è un omomorfismo di moduli graduati $f\colon C \to C'$ di grado 0 tale che $d'f = fd$, mentre una *omotopia* h tra due mappe di catene f e g è un omomorfismo di moduli graduati tra C e C' di grado 1 per cui si abbia $d'h + hd = f - g$. Diciamo inoltre che f è omotopa a g se esiste una tale omotopia tra f e g.

Definizione 4. Una mappa di catene $f\colon C \to C'$ è detta *equivalenza omotopica* se esiste una mappa di catene $f'\colon C' \to C$ tale che $f'f \simeq \mathrm{id}_C$ e $ff' \simeq \mathrm{id}'_C$. Un complesso di catene C è detto invece *contraibile* se id_C è omotopicamente equivalente alla mappa di catene nulla.

Più in generale possiamo considerare risoluzioni proiettive:

Definizione 5. Sia A un R-modulo; una *risoluzione proiettiva* di A è un complesso di catene

$$\dots \longrightarrow P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \longrightarrow 0$$

tale che:

- I P_j sono R-moduli proiettivi;
- $H_0(P) \simeq A$;
- La successione è esatta in P_i per ogni $i > 0$.

Per risoluzioni proiettive vale infatti il seguente lemma di fondamentale importanza per la definizione dei gruppi di omologia e coomologia:

Lemma 6. *Siano (C,d) e (C',d') due complessi di catene con C proiettivo e D aciclico. Allora per ogni mappa $f\colon \mathrm{H}_0(C) \to \mathrm{H}_0(D)$ esiste una mappa di catene $F\colon C \to C'$ che estende f, e tale F è unica a meno di omotopia.*

Corollario 7. *Due risoluzioni proiettive di A hanno lo stesso tipo di omotopia.*

2. G-moduli

Ai fini della coomologia dei gruppi, siamo particolarmente interessati al caso in cui l'anello dei coefficienti R è un anello gruppo:

Definizione 8. Sia G un gruppo fissato. Chiamiamo *anello gruppo* lo $\mathbb{Z}$-modulo libero generato dagli elementi di G, indicato con $\mathbb{Z}[G]$ o $\mathbb{Z}G$.

L'anello gruppo $\mathbb{Z}[G]$ consiste delle somme formali $\sum_{g\in G} \alpha(g)g$, dove $\alpha(g)$ è diverso da 0 solo per un numero finito di $g \in G$; una base è data proprio dall'insieme degli elementi di G, su cui è ancora ben definito il prodotto iniziale. Tale prodotto si può allora estendere linearmente a tutte le coppie di elementi del modulo nel seguente modo:

$$\left(\sum_{g\in G}\alpha(g)g\right)\left(\sum_{h\in G}\alpha(h)h\right)=\sum_{g,h\in G}(\alpha(g)\alpha(h))gh$$

Si può verificare che con questo prodotto $\mathbb{Z}[G]$ diventa un anello, e che il suo gruppo moltiplicativo $(\mathbb{Z}[G])^*$ contiene G come sottogruppo. Più precisamente, vale la seguente proprietà universale:

Proposizione 9. *Sia $i\colon G\to\mathbb{Z}[G]$ l'immersione, ed R un anello. Per ogni mappa $f\colon G\to R$ per cui $f(xy)=f(x)f(y)$ e $f(1)=1_R$, esiste un unico omomorfismo di anelli $\tilde{f}\colon\mathbb{Z}[G]\to R$ tale che $\tilde{f}i=f$.*

Dimostrazione. Definiamo $\tilde{f}(\sum_{g\in G}\alpha(g)g)=\sum_{g\in G}\alpha(g)f(g)$, e questo è l'unico omomorfismo di anelli che estende f. □

Diamo ora alcuni esempi di anello gruppo:

Esempio.
(1) Sia G un gruppo ciclico di ordine n, e sia t un suo generatore. Una base di $\mathbb{Z}[G]$ è data dall'insieme delle potenze $t^0,\dots,t^{n-1}$; poiché vale in G la relazione $t^n=1$, otteniamo che l'anello gruppo su G è isomorfo all'anello di polinomi $\mathbb{Z}[T]/(T^n-1)$.
(2) Se G è un gruppo ciclico infinito, allora una base di $\mathbb{Z}[G]$ è data da tutte le potenze del generatore t, ovvero $\{t^i\}_{i\in\mathbb{Z}}$; allora $\mathbb{Z}G\simeq\mathbb{Z}[T,T^{-1}]$, polinomi di Laurent a coefficenti in $\mathbb{Z}$.

Poiché $\mathbb{Z}[G]$ ha una struttura di anello, ha senso considerare degli $\mathbb{Z}G$-moduli, che scriveremo, più semplicemente, G-moduli. Un G-modulo è allora un gruppo abeliano A con un omomorfismo di anelli di $\mathbb{Z}[G]$ in $\mathrm{End}(A)$. Dalla proprietà universale sappiamo però che:

$$\mathrm{Hom}_{(anelli)}(\mathbb{Z}G,R)\simeq\mathrm{Hom}_{(gruppi)}(G,R^*)$$

dunque un tale omomorfismo di anelli corrisponde ad un omomorfismo di gruppi di G in $\mathrm{Aut}(A)$, ovverosia un'azione di G su A.

Diciamo che A ha struttura di G-modulo banale se l'azione di G su A è quella banale, ovvero $ga=a$ per ogni $g\in G$ e $a\in A$. Osserviamo che in tal caso tale azione si estende per la proprietà universale all'azione

$$ra=\varepsilon(r)a\quad\forall r\in\mathbb{Z}[G]\quad\forall a\in A$$

dove l'omomorfismo di anelli ε è detto, in analogia al caso dei complessi di catene, *mappa di aumentazione*, ed è tale che $\varepsilon\colon\mathbb{Z}G\to\mathbb{Z}$, $\varepsilon(g)=1$ per ogni $g\in G$.

In particolare, possiamo considerare anche $\mathbb{Z}$ come un G-modulo banale. Il prossimo passo è allora trovare delle risoluzioni libere di $\mathbb{Z}$ tramite $\mathbb{Z}G$-moduli.

3. Risoluzioni di $\mathbb{Z}$

Come accennato nella sezione precedente, nel seguito pensiamo $\mathbb{Z}$ come G-modulo banale. Costruiremo le risoluzioni libere cercate a partire da azioni libere di G su un complesso cellulare contraibile.

Cominciamo dal considerare un insieme X ed un'azione di G sui suoi elementi. Possiamo formare il gruppo abeliano libero generato da X e indicato con $\mathbb{Z}[X]$, ed estendere l'azione di G in modo

$\mathbb{Z}$-lineare su $\mathbb{Z}[X]$. Otteniamo in tal modo una struttura di G-modulo su $\mathbb{Z}[X]$, e ciò fatto si può fare per ogni insieme X; in particolare possiamo considerare come supporto l'insieme dei coset di un sottogruppo H di G, dove l'azione di G su X è data dalla moltiplicazione a sinistra.

Poiché X si decompone in unione disgiunta delle orbite di G, e si ha facilmente che

$$\mathbb{Z}[\sqcup X_i] = \oplus \mathbb{Z}[X_i]$$

segue che $\mathbb{Z}[X]$ ammette una decomposizione come somma diretta di $\mathbb{Z}[\mathrm{Orb}(x)]$, con x che varia su un insieme di rappresentanti delle G-orbite. Osserviamo inoltre che l'orbita di $x \in X$ è in corrispondenza biunivoca con l'insieme dei cosets di $\mathrm{Stab}(x)$ in G, e dunque

$$\mathbb{Z}[X] \simeq \oplus \mathbb{Z}[G/\mathrm{Stab}(x)]$$

In particolare, se G agisce in modo libero, $\mathrm{Stab}(x)$ è banale, e abbiamo ottenuto la seguente proposizione:

Proposizione 10. *Sia X un insieme su cui G agisce liberamente, ed E l'insieme dei rappresentanti delle G-orbite in X. Allora $\mathbb{Z}[X]$ è uno $\mathbb{Z}G$-modulo libero con base E.*

Sia ora X un CW-complesso e supponiamo che G agisca sulla struttura cellulare di X permutandone le celle, ovvero chiediamo che ad ogni $g \in G$ corrisponda un omeomorfismo $x \mapsto gx$ di X tale che l'immagine $g\sigma$ di ogni cella σ sia ancora una cella di X.

Definizione 11. Chiamiamo *G-complesso* un CW-complesso X con un'azione di G che ne permuta le celle.

Se X è un G-complesso, allora l'azione di G su X induce un'azione di G sul complesso di catene cellulare associato ad X, che indichiamo con $C_*(X)$. Infatti ogni $C_k(X)$ è uno $\mathbb{Z}$-modulo libero la cui base è in corrispondenza biunivoca con le k-celle di X; l'azione di G, permutando queste celle, induce allora un'azione sugli elementi della base di $C_k(X)$, azione che si estende in modo $\mathbb{Z}$-lineare, dotando $C_k(X)$ della struttura di $\mathbb{Z}G$-modulo. Poiché anche la mappa di aumentazione $\varepsilon\colon C_0(X) \to \mathbb{Z}$ è anch'essa una mappa di G-moduli, abbiamo ottenuto una successione di $\mathbb{Z}G$-moduli che è il candidato ideale per una risoluzione libera di $\mathbb{Z}$. Resta infatti da controllare che tale successione sia libera, cosa che però non è vera in generale, e ad omologia nulla.

Diciamo che X è un *G-complesso libero* se l'azione di G su X permuta liberamente le celle, nel senso che $g\sigma \neq \sigma$ per ogni cella σ del complesso e per ogni elemento non banale di G. Osserviamo allora che se il complesso X è anche libero, ogni modulo $C_n(X)$, visto come gruppo abeliano libero generato dalle n-celle, ha una base che è permutata liberamente da G; quindi, per la proposizione precedente, $C_n(X)$ risulta essere uno $\mathbb{Z}G$-modulo libero con un elemento della base per ogni G-orbita delle celle.

Infine, se X è contraibile, allora ha omologia aumentata nulla, da cui la successione di $\mathbb{Z}[G]$-moduli

$$\dots \longrightarrow C_n(X) \xrightarrow{\partial_n} \dots \xrightarrow{\partial_2} C_1(X) \xrightarrow{\partial_1} C_0(X) \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

è esatta, e risulta essere una risoluzione libera di $\mathbb{Z}$. Abbiamo dimostrato il seguente teorema:

Teorema 12. *Sia X un G-complesso libero contraibile. Allora il complesso di catene aumentato è una risoluzione libera di $\mathbb{Z}$ in $\mathbb{Z}[G]$-moduli.*

Corollario 13. *Se Y è un CW-complesso, che è anche un $K(G,1)$, allora il complesso di catene aumentato relativo al rivestimento universale è una risoluzione libera di $\mathbb{Z}$ in $\mathbb{Z}G$-moduli. Esso infatti è un CW-complesso contraibile, su cui G agisce liberamente.*

Possiamo dare finalmente un esempio di una risoluzione libera di $\mathbb{Z}$:

Esempio. Siano $G = F(S)$ il gruppo libero generato da un insieme S ed Y il bouquet su $|S|$ circonferenze. Allora Y è un $K(F(S),1)$ che è anche un CW-complesso, (con la struttura cellulare data da una 0-cella y_0 ed $|S|$ 1-celle). La 0-cella $\tilde{y}_0$ rappresenta l'unica G-orbita dei vertici del rivestimento universale X, e quindi genera lo $\mathbb{Z}G$-modulo libero $C_0(X)$. Come base per $C_1(X)$ prendiamo invece, per ogni $s \in S$, una 1-cella orientata e_s di X con immagine in S^1_s. A meno di sostituire e_s con ge_s per un opportuno $g \in G$, possiamo supporre che e_s abbia punto base $\tilde{y}_0$. Il punto finale è dato allora da sy_0, quindi si ha $\partial e_s = sy_0 - y_0 = (s-1)y_0$ (a meno di identificare $\tilde{y}_0$ con $1 \in \mathbb{Z}G$). La risoluzione libera ottenuta è perciò:

$$0 \longrightarrow \mathbb{Z}G^{|S|} \xrightarrow{\partial} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

Osserviamo che se S è ciclico infinito, generato da t, allora la risoluzione diventa

$$0 \longrightarrow \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{1}$$

4. Definizione di H_*G e H^*G

Abbiamo finalmente gli strumenti per dare il concetto di omologia e coomologia di un gruppo G.

Fissiamo a questo scopo un G-modulo M, e chiamiamo M_G il quoziente di M per il sottoodulo generato dagli elementi della forma $gm - m$, con $g \in G$ e $m \in M$.

Un'utile descrizione di M_G viene dal prodotto tensore $\mathbb{Z} \otimes_{\mathbb{Z}G} M$, dove $\mathbb{Z}$ è visto come G-modulo destro banale ed M come G-modulo sinistro. Osserviamo infatti, che in questo prodotto tensore si hanno le relazioni:

$$1 \otimes_G gm = 1g \otimes_G m = 1 \otimes_G m$$

per ogni $g \in G$ e ogni $m \in M$. Quindi

$$\mathbb{Z} \otimes_G M = \frac{\mathbb{Z} \otimes_{\mathbb{Z}} M}{\langle 1 \otimes gm - 1 \otimes m \rangle} \simeq \frac{M}{gm - m} = M_G$$

Scrivere M_G come un prodotto tensore, implica le due proprietà seguenti:

(1) Se la successione $M' \to M \to M'' \to 0$ è esatta, anche la successione indotta $M'_G \to M_G \to M''_G \to 0$ è esatta;
(2) Se F è uno $\mathbb{Z}[G]$-modulo libero con base (e_i), allora F_G è uno $\mathbb{Z}$-modulo libero di base $(\overline{e}_i)$.

Proposizione 14. *Sia X un G-complesso libero. Allora $(C_*(X))_G \simeq C_*(X/G)$*

Dimostrazione. La proiezione $\pi\colon C_n(X) \to C_n(X/G)$ induce, per passaggio al quoziente, una mappa di $\mathbb{Z}$-moduli $\phi\colon (C_n(X))_G \to C_n(X/G)$. Inoltre, $(C_n(X))_G$ e $C_n(X/G)$ hanno una base come $\mathbb{Z}$-moduli, data da un elemento per ogni G-orbita delle celle di X, e la mappa ϕ manda ogni elemento della base di $(C_n(X))_G$ nel rispettivo elemento della base di $C_n(X/G)$. Ciò mostra che ϕ è un isomorfismo. □

Sia G un gruppo ed $\varepsilon\colon P \to \mathbb{Z}$ una risoluzione proiettiva di $\mathbb{Z}$ in $\mathbb{Z}G$-moduli.

Definizione 15. Definiamo gruppo di omologia di G il gruppo graduato

$$\mathrm{H}_i(G) = \mathrm{H}_i(P_G)$$

Osserviamo, che per il lemma (6), il secondo membro dell'uguaglianza non dipende dalla risoluzione proiettiva scelta, e dunque quella data è una buona definizione.

Una definizione equivalente di omologia di un gruppo G è data come omologia del suo spazio classificante:

$$\mathrm{H}_i(G) = \mathrm{H}_i(\mathrm{K}(G,1), \mathbb{Z})$$

Infatti, la seguente proposizione ci mostra come le due definizioni date coincidano:

Proposizione 16. *Se Y è un CW-complesso che è un $\mathrm{K}(G,1)$ allora $\mathrm{H}_*(G) \simeq \mathrm{H}_*(Y)$.*

Dimostrazione. Abbiamo già visto che se Y è un CW-complesso ed un $\mathrm{K}(G,1)$, di rivestimento universale X, allora il complesso cellulare $C_*(X)$ dà una risoluzione libera di $\mathbb{Z}$. Poiché per la proposizione precedente $(C_*(X))_G \simeq C_*(Y)$, si ha allora la tesi. □

Esempio.
(1) Sia Y il bouquet di circonferenze indicizzato dall'insieme S.
Allora Y è un $\mathrm{K}(F(S),1)$ e:

$$\mathrm{H}_i(F(S)) = \begin{cases} \mathbb{Z} & \text{per } i = 0 \\ \mathbb{Z}[S] & \text{per } i = 1 \\ 0 & \text{altrimenti} \end{cases}$$

(2) Sia S_g la superficie di genere g e $G = \pi_1(S_g, x_0) \simeq \langle a_1, \dots, a_g, b_1, \dots, b_g \mid \prod_{i=1}^{g}[a_i, b_i]\rangle$. Poiché il rivestimento universale di S_g è $\mathbb{R}^2$ per $g = 0$ e il piano iperbolico $\mathbb{H}^2$ per $g \neq 0$, entrambi contraibili, si ha che S_g è un $\mathrm{K}(G,1)$, e di conseguenza:

$$\mathrm{H}_i(G) = \mathrm{H}_i(S_g) = \begin{cases} \mathbb{Z} & \text{per } i = 0, 2 \\ \mathbb{Z}^{2g} & \text{per } i = 1 \\ 0 & \text{altrimenti} \end{cases}$$

Più in generale, possiamo definire l'omologia, e la coomologia di un gruppo a coefficenti in un arbitrario G-modulo M. Per farlo, seguendo le orme dettate dall'omologia a coefficenti in $\mathbb{Z}$ consideriamo una risoluzione proiettiva F di $\mathbb{Z}$ in $\mathbb{Z}G$-moduli;

Definizione 17. Chiamiamo *omologia di G a coefficenti in M* l'omologia del complesso $F \otimes_G M$, ovvero

$$\mathrm{H}_*(G, M) = \mathrm{H}_*(F \otimes_G M)$$

Chiaramente la definizione appena data è una generalizzazione della precedente, in quanto, prendendo $M = \mathbb{Z}$ si ha $\mathrm{H}_*(G, \mathbb{Z}) = \mathrm{H}_*(F \otimes_G \mathbb{Z}) = \mathrm{H}_*(F_G) = \mathrm{H}_*(G)$. Anche in tal caso, il secondo membro non dipende dalla risoluzione proiettiva scelta, e dunque $\mathrm{H}_*(G, M)$ risulta essere ben definito.

Esempio. Vediamo che $\mathrm{H}_0(G,M) \simeq M_G$.

Dire che $\dots \to F_1 \to F_0 \to \mathbb{Z} \to 0$ è una risoluzione significa, in particolare, che è una successione esatta.

Tensorizziamo otteniamo allora che la successione $\dots \to F_1 \otimes_G M \to F_0 \otimes_G M \to \mathbb{Z} \otimes_G M \to 0$ è ancora esatta. Possiamo dunque calcolare l'omologia della risoluzione $\dots \to F_1 \otimes_G M \to F_0 \otimes_G M \to 0$ sfruttando le proprietà di esattezza:

$$\mathrm{H}_0(G,M) = \frac{F_0 \otimes_G M}{\mathrm{Im}(\partial_1 \otimes \mathrm{id})} \simeq \frac{F_0 \otimes_G M}{\ker(\varepsilon \otimes \mathrm{id})} \simeq \mathbb{Z} \otimes_G M = M_G.$$

Analogamente a quanto fatto fino ad ora, possiamo definire il concetto di coomologia di un gruppo G; fissata sempre una determinata risoluzione proiettiva $\varepsilon \colon F \to \mathbb{Z}$ di $\mathbb{Z}$, passiamo ai duali $\mathrm{Hom}_{\mathbb{Z}G}(-,M)$:

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},M) \xrightarrow{\varepsilon^*} \mathrm{Hom}_{\mathbb{Z}G}(F_0,M) \xrightarrow{\partial_1^*} \mathrm{Hom}_{\mathbb{Z}G}(F_1,M) \xrightarrow{\partial_2^*} \dots$$

Definizione 18. Chiamiamo *coomologia di G a coefficenti in M* la coomologia del complesso di cocatene $\mathrm{Hom}_{\mathbb{Z}G}(F,M)$, ovvero:

$$\mathrm{H}^*(G,M) = \mathrm{H}^*(\mathrm{Hom}_{\mathbb{Z}G}(F,M))$$

Osserviamo che, ancora una volta, se F è una risoluzione proiettiva di $\mathbb{Z}$, la definizione appena data è buona. Inoltre $\mathrm{H}^0(G,M) = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)$, e se poniamo

$$M^G = \{m \in M \mid gm = m \ \forall g \in G\}$$

si ha che $\mathrm{H}^0(G,M) = M^G$.

Infatti, se $\phi \colon \mathbb{Z} \to M$ è un omomorfismo, allora è identificato dall'immagine $\phi(1) = m$ di $1 \in \mathbb{Z}$. Se però $\phi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)$, allora

$$gm = \phi(g1) = \phi(1) = m \quad \forall g \in G$$

Dunque ϕ è un omomorfismo di G-moduli se e solo se $\phi(1)$ resta fissato dall'azione di G, ovvero la tesi.

Esempio. Sia G gruppo ciclico infinito di generatore t, caso in cui si è vista la risoluzione (1); allora $\mathrm{H}_*(G,M)$ è l'omologia del complesso

$$\dots \longrightarrow 0 \longrightarrow \mathbb{Z}G \otimes_G M \simeq M \xrightarrow{\mathrm{id}\otimes(t-1)} \mathbb{Z}G \otimes_G M \simeq M$$

mentre $\mathrm{H}^*(G,M)$ è la coomologia del complesso

$$\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,M) \simeq M \xrightarrow{t-1} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,M) \simeq M \longrightarrow 0 \longrightarrow \dots$$

e quindi $\mathrm{H}_0(G,M) = \mathrm{H}^1(G,M) = M_G, \mathrm{H}_1(G,M) = \mathrm{H}^0(G,M) = M^G$, $\mathrm{H}_i(G,M) = \mathrm{H}^i(G,M) = 0$ per $i > 1$.

Osservazione 19. Se M è un G-modulo banale, allora $\mathrm{H}^*(G,M)$ coincide con $\mathrm{H}^*(Y)$ dove Y è un $\mathrm{K}(G,1)$. Infatti il complesso di catene del rivestimento universale X di Y dà una risoluzione libera di $\mathbb{Z}$, e applicando il funtore $\mathrm{Hom}_G(-,M)$ possiamo calcolare $\mathrm{H}^*(G,M)$ come $\mathrm{H}^*(C^*(X),M)$. Osserviamo ora, che se l'azione di G su M è banale, allora

$$\mathrm{Hom}_G(C_n(X),M) \simeq \mathrm{Hom}_{\mathbb{Z}}(C_n(Y),M)$$

Infatti, se $\phi\colon C_n(X) \to M$ è una n-cocatena, allora $\phi(g\sigma) = \phi(\sigma)$ per ogni $g \in G$; quindi ϕ si fattorizza ad un $\mathbb{Z}$-omomorfismo di $C_n(Y)$ in M.

Osservazione 20. Se l'azione di G su M non è quella banale, $\mathrm{H}_*(G, M)$ e $\mathrm{H}^*(G, M)$ hanno ancora un rispettivo topologico come omologia (o coomologia) dello spazio classificante $\mathrm{K}(G, 1)$ a coefficienti locali.

5. Risoluzione standard

Per dare altri esempi di calcolo di gruppi di omologia e coomologia è conveniente introdurre una risoluzione a partire dal gruppo stesso, usando come complesso di catene C_* il complesso dei simplessi ordinati di G. Più precisamente, sia $F_n = C_n(G)$ lo $\mathbb{Z}$-modulo libero generato dalle $(n+1)$-uple ordinate di elementi di G, $(g_0, \dots, g_n)$; in questo caso, poiché il gruppo G agisce su sé stesso per moltiplicazione a sinistra l'azione che considereremo è data da $g(g_0, \dots, g_n) = (gg_0, \dots, gg_n)$. In tal modo F_n è anche uno $\mathbb{Z}G$-modulo libero per ogni $n \in \mathbb{N}$.

L'operatore di bordo $\partial_n\colon F_n \to F_{n-1}$ è dato da

$$\partial_n = \sum_{i=0}^{n} (-1)^i d_i$$

dove $d_i(g_0, \dots, g_n) = (g_0, \dots, \hat{g}_i, \dots, g_n)$.

Se $\varepsilon\colon F_0 \simeq \mathbb{Z}[G] \to \mathbb{Z}$ è la solita mappa di aumentazione, abbiamo ottenuto una successione di G-moduli liberi. Se verifichiamo che è anche un complesso aciclico, abbiamo ottenuto una nuova risoluzione libera di $\mathbb{Z}$.

Definiamo a questo scopo l'omomorfismo di gruppi abeliani $h\colon F_* \to F_{*+1}$ ponendo $h(g_0, \dots, g_n)$ pari a $(1, g_0, \dots, g_n)$ se $n \geq 0$, e $h(1) = 1$ se $n = -1$; essa è tale che $h\partial_* + \partial_{*+1}h = \mathrm{id}$ in quanto:

$$\begin{aligned}
(\partial_{n+1}h_n + h_{n-1}\partial_n)(y_0, \dots, y_n) &= \partial_{n+1}(1, y_0, \dots, y_n) + h_{n-1}\left(\sum_{h=0}^{n} (-1)^h (y_0, \dots, \hat{y}_h, \dots, y_n)\right) \\
&= (y_0, \dots, y_n) + \sum_{h=0}^{n} (-1)^{h+1} (1, y_0, \dots, \hat{y}_h, \dots, y_n) \\
&+ \sum_{h=0}^{n} (-1)^h (1, y_0, \dots, \hat{y}_h, \dots, y_n) \\
&= (y_0, \dots, y_n)
\end{aligned}$$

e dunque è un'omotopia tra l'identità di F_* e la mappa nulla. Il complesso così definito è dunque aciclico.

Definizione 21. Chiamiamo *risoluzione standard di $\mathbb{Z}$ per $\mathbb{Z}[G]$-moduli* la risoluzione libera così ottenuta.

Osserviamo che una base di F_n come $\mathbb{Z}[G]$-modulo è data dalle $(n+1)$-uple con primo elemento pari a 1. Infatti questi elementi generano F_n in quanto $(y_0, \dots, y_n) = y_0(1, y_0^{-1}y_2, \dots, y_0^{-1}y_n)$, e se si avesse una relazione non banale

$$0 = \sum_{i=1}^{n} \left(\sum_{g \in G} \alpha(g)_i g \right) (1, y_1^i, \dots, y_n^i) = \sum_{g \in G, i=0}^{n} \alpha(g)_i (g, g y_1^i, \dots, g y_n^i)$$

otterremmo che tutti gli elementi $(g, gy_1^i, \dots, gy_n^i)$ sono distinti, perché lo sono le prime coordinate. Dunque gli $\alpha(g)_i$ sono tutti nulli, contro l'ipotesi di relazione non banale.

È conveniente utilizzare la seguente *bar-resolution*: scriviamo una $(n+1)$-upla nella forma

$$(1, g_1, g_1 g_2, \dots, g_1 g_2 \cdots g_n) =: [g_1 | \dots | g_n].$$

Osserviamo che se $n = 0$, vi è un solo elemento, dato da $[\quad]$ e d'ora in avanti identificato con $1 \in \mathbb{Z}G$.

Il morfismo di bordo, scritto in termini della base, è ancora dato da $\partial_n = \sum_{i=0}^{n} (-1)^i d_i$, ma questa volta

$$d_i [g_1 | \dots | g_n] = \begin{cases} g_1 [g_2 | \dots | g_n] & \text{per } i = 0 \\ [g_1 | \dots | g_{i-1} | g_i g_{i+1} | g_{i+2} | \dots | g_n] & \text{per } 0 < i < n \\ [g_1 | \dots | g_{n-1}] & \text{per } i = n \end{cases}$$

Per il seguito sarà utile considerare la risoluzione standard *normalizzata* $\overline{F}_* = F_* / D_*$, dove il complesso D_* è il sottocomplesso di F_* generato dagli elementi $(g_0, \dots, g_n)$ tali che $g_i = g_{i+1}$ per qualche i. In questo modo l'operatore di bordo passa al quoziente, definendo un complesso di catene. In termini della *bar-resolution* osserviamo che D_* è il G-sottocomplesso di F_* generato dagli elementi $[g_1 | \dots | g_n]$ per cui $g_i = 1$ per qualche indice i. Quindi $\overline{F}_*$ è lo $\mathbb{Z}G$-modulo libero con un elemento della base per ogni n-upla di elementi non banali di G. Poiché l'omotopia h vista sopra manda D_* in sé, essa induce un'omotopia tra $\overline{F}_*$ e la risoluzione nulla, e dunque è ancora una risoluzione libera.

Esempio (Risoluzioni periodiche). Sia X un G-complesso omeomorfo alla sfera S^{2n-1} e sia G un gruppo che agisce liberamente sulle celle di X. Poiché X è compatto, ammette un numero finito di 0-celle, e su queste G agisce in modo libero; allora G deve essere finito.

Per il teorema del punto fisso di Lefshetz, ogni elemento $g \in G$ ha numero di Lefshetz $\tau(g) = 0$, dove ricordiamo che

$$\tau(f) = \sum_n (-1)^n \mathrm{tr}(f_* \colon \mathrm{H}_n(X) \to \mathrm{H}_n(X))$$

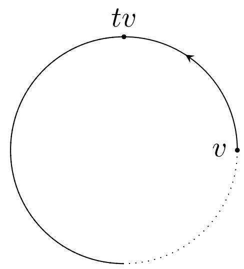
ovvero la somma a segni alterni della traccia degli omomorfismi indotti in omologia. Poiché l'omologia di X è quella della sfera S^{2n-1}, allora gli unici gruppi non nulli sono $\mathrm{H}_0(X) \simeq \mathrm{H}_{2n-1}(X) \simeq \mathbb{Z}$, e poiché l'omomorfismo indotto a livello 0 è l'identità, otteniamo che anche quello a livello $2n-1$ è l'omomorfismo identico. Ciò vuol dire che G agisce in modo banale su $\mathrm{H}_{2n-1}(X)$, e quindi la seguente successione risulta essere esatta:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\eta} C_{2n-1}(X) \longrightarrow \dots \longrightarrow C_1(X) \longrightarrow C_0(X) \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{2}$$

In più, ogni componente $C_i(X)$ della successione è libero. Mettendo insieme infinite copie di questa successione esatta, otteniamo allora una risoluzione libera di $\mathbb{Z}$ per mezzo di $\mathbb{Z}G$-moduli, che è anche periodica di periodo $2n$:

$$\dots \longrightarrow C_0(X) \xrightarrow{\eta\varepsilon} C_{2n-1}(X) \longrightarrow \dots \longrightarrow C_0(X) \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

Nel caso in cui G è ciclico di ordine n e generatore t, possiamo prendere come azione di G quella data dalle rotazioni su S^1, quest'ultimo visto come CW-complesso formato da n vertici ed n 1-celle. Supponiamo, ad esempio che queste 1-celle siano tutte immagini di e:



Allora $\mathrm{H}_1(S^1)$ è generato dal ciclo $e + te + t^2e + \cdots + t^{n-1}e = Ne$, dove per comodità si è posto $N = 1 + t + t^2 + \cdots + t^{n-1} \in \mathbb{Z}G$; la successione (2) assume allora la forma

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\eta} \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

dove $\eta(1) = N$ ed $\varepsilon(1) = 1$. Da qui si ha dunque la risoluzione periodica:

$$\dots \longrightarrow \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{3}$$

6. Omologia e coomologia dei gruppi ciclici finiti

Sia G il gruppo ciclico di ordine n su generaore t; dalla risoluzione (3), valida per i gruppi ciclici, tensorizzando otteniamo:

$$\dots \xrightarrow{\mathrm{id}\otimes(t-1)} \mathbb{Z} \otimes_G \mathbb{Z}G \xrightarrow{\mathrm{id}\otimes N} \mathbb{Z} \otimes_G \mathbb{Z}G \xrightarrow{\mathrm{id}\otimes(t-1)} \mathbb{Z} \otimes_G \mathbb{Z}G \longrightarrow 0$$

Osserviamo ora che $\mathbb{Z} \otimes_G \mathbb{Z}G \simeq \mathbb{Z}$ e che si hanno le seguenti relazioni:

$$(\mathrm{id} \otimes (t-1))(1 \otimes_G g) = 1 \otimes_G (t-1)g = 1 \otimes_G tg - 1 \otimes_G g = 1 \otimes_G g - 1 \otimes_G g = 0$$

$$(\mathrm{id} \otimes (N))(1 \otimes_G g) = 1 \otimes_G (1 + t + t^2 + \cdots + t^{n-1})g = n(1 \otimes_G g).$$

Allora il calcolo dell'omologia di G si riduce a calcolare l'omologia del complesso

$$\dots \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \longrightarrow 0$$

data da:

$$\mathrm{H}_i(G) = \begin{cases} \mathbb{Z} & \text{per } i = 0 \\ \mathbb{Z}_n & \text{per } i \text{ dispari} \\ 0 & \text{per } i \text{ pari positivo} \end{cases}$$

Calcoliamo ora la sua coomologia a coefficenti interi, sempre a partire dalla risoluzione (3). Applicando il funtore $\mathrm{Hom}_G(-, \mathbb{Z})$ otteniamo:

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, \mathbb{Z}) \xrightarrow{(t-1)^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, \mathbb{Z}) \xrightarrow{N^*} \dots$$

Osserviamo ora che $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, \mathbb{Z}) \simeq \mathbb{Z}$, e resta solo da capire chi sono le mappe $(t-1)^*$ e N^*; sia dunque $\phi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, \mathbb{Z})$.

$$(t-1)^*(\phi)(1) = \phi((t-1)(1)) = \phi(t-1) = t\phi(1) - \phi(1) = \phi(1) - \phi(1) = 0$$

Analogamente, $N^*(\phi)(1) = \phi(\sum_{h=0}^{n-1} t^h) = n\phi(1)$. Il complesso si riscrive allora come:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\;0\;} \mathbb{Z} \xrightarrow{\;n\;} \dots$$

e la coomologia di G risulta essere:

$$\mathrm{H}^i(G, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{per } i = 0 \\ \mathbb{Z}_n & \text{per } i \text{ pari positivo} \\ 0 & \text{altrimenti} \end{cases}$$

7. Ampliamenti di gruppi

Definizione 22. Chiamiamo *estensione* o *ampliamento* di G per un gruppo N una sequenza esatta corta di gruppi (scitti in notazione moltiplicativa)

$$1 \longrightarrow N \xrightarrow{\;\iota\;} E \xrightarrow{\;\pi\;} G \longrightarrow 1$$

Diciamo che due estensioni di G per N sono equivalenti se esiste una mappa $\psi \colon E \to E'$ che fa commutare il seguente diagramma:

$$\begin{tikzcd} & & E \arrow[dd, dashed, "\psi"] \arrow[dr, "\pi"] & & \\ 1 \arrow[r] & N \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & & G \arrow[r] & 1 \\ & & E' \arrow[ur, "\pi'"'] & & \end{tikzcd}$$

Osserviamo, in particolare, che per il lemma dei 3 ψ deve essere un isomorfismo.

Studiamo ora il problema della classificazione di tali estensioni nel caso in cui N sia un sottogruppo abeliano di E, e per sottolineare tale ipotesi denoteremo più suggestivamente con A, in notazione additiva, il gruppo con cui vogliamo ampliare G. In tal caso l'estensione corrispondente

$$0 \longrightarrow A \xrightarrow{\;\iota\;} E \xrightarrow{\;\pi\;} G \longrightarrow 1$$

induce un'azione di G su A, rendendo A un G-modulo. Infatti su $\iota(A)$ E agisce per coniugio, e poiché A (e dunque $\iota(A)$ è un gruppo abeliano, l'azione per coniugio ristretta a $\iota(A)$ coincide con l'azione banale. Ciò rende allora ben definita l'azione di E/A, ovvero di G su A. Per ogni $g \in G$ fissiamo infatti un rappresentante $\tilde{g} \in X$, con $\pi(\tilde{g}) = g$; l'azione di g si scrive come azione di coniugio per $\tilde{g}$, ovvero:

$$i(ga) = \tilde{g} i(a) \tilde{g}^{-1}$$

che possiamo riscrivere come

$$\tilde{g} i(a) = i(ga) \tilde{g}$$

Vediamo infatti che questa appena definita è effettivamente un'azione, ovvero che $hg(a) = h(g(a))$ per ogni $g, h \in G$ (è chiaro che $\mathrm{id}(a) = a$). Fissiamo a questo scopo, per comodità di notazione, una sezione s di π in modo che $\pi(s(g)) = g$ per ogni $g \in G$. In tal caso $hg = \pi(s(hg))$, $h = \pi(s(h))$ e $g = \pi(s(g))$; dunque $\pi(s(hg)) = hg = \pi(s(h))\pi(s(g))$ e poiché π è un omomorfismo, $s(hg)s^{-1}(h)s^{-1}(g) \in \ker(\pi) = \mathrm{Im}(\iota)$, quindi diciamo essere uguale a $\iota(a')$. Sfruttando il fatto che A è abeliano, si ha

$$\begin{aligned}\iota((hg)a) = s(hg)\iota(a)s^{-1}(hg) &= s(h)s(g)\iota(a')\iota(a)(\iota(a'))^{-1}s(g)^{-1}s(h)^{-1} \\ &= s(h)s(g)\iota(a)s(g)^{-1}s(h)^{-1} = \iota(h(g(a)))\end{aligned}$$

Vediamo ora che l'azione scelta non dipende dal rappresentante; sia allora t un'altra sezione di π, ovvero per ogni $g \in G$ si ha $\pi(s(g)) = g = \pi(t(g))$. Sempre perché π è un omomorfismo, $t(g)^{-1}s(g) = \iota(a')$ e quindi

$$s(g)\iota(a)(s(g))^{-1} = t(g)\iota(a')\iota(a)(\iota(a'))^{-1}(t(g))^{-1} = t(g)\iota(a)(t(g))^{-1}$$

e quindi l'azione è ben definita.

Data la struttura di G-modulo su A, possiamo raffinare il problema della classificazione delle estensioni cercando gli ampliamenti di G tramite A che inducono l'azione fissata di G su A, a meno di equivalenza.

Osservazione 23. È facile verificare che estensioni equivalenti inducono la stessa azione di G su A e ciò verrà usato nel seguito senza altra specificazione.

Cominciamo lo studio fissando un G-modulo A ed una sezione s come sopra. Non è detto che s sia un omomorfismo; possiamo però supporre, per semplicità, che

$$s(1) = 1 \qquad \text{(condizione di normalizzazione)}$$

cosa peraltro vera nel caso in cui s sia un omomorfismo.

Per ogni g, h in G possiamo considerare gli elementi $s(g)s(h)$ e $s(gh)$. Se s è un omomorfismo, si ha $s(g)s(h) = s(gh)$, mentre nel caso generale, poiché $\pi(s(g)s(h)) = \pi(s(gh)) = gh$ per ogni g, $h \in G$, e poiché la successione (7) è esatta, essi differiscono per un elemento di $i(A)$. Possiamo allora porre:

$$s(g)s(h) = i(f(g,h))s(gh)$$

dove $f\colon G \times G \to A$ è una funzione che dipende dalla coppia (g, h), e misura quanto s si discosti dall'essere un omomorfismo. Dalla condizione di normalizzazione, otteniamo che $s(g) = s(g)s(1) = \iota(f(g, 1))s(g)$, ovvero

$$f(g, 1) = f(1, g) = 0 \tag{4}$$

per ogni $g \in G$. Diciamo in tal caso che f è *normalizzata*.

Il nostro obiettivo è mostrare che l'estensione di partenza è determinata dalla struttura di G-modulo di A e dalla funzione f. Sia a questo scopo $s(G)$ l'immagine di G in E. Questo è un insieme di rappresentanti dei coset di $\iota(A)$ in E, perché $E/\iota(A) \simeq G$. Abbiamo allora una bigezione tra $A \times G$ ed E data da $(a, g) \mapsto \iota(a)s(g)$.

L'idea è ora quella di calcolare la legge di gruppo su $A \times G$ per rendere i due gruppi isomorfi:

$$(a, g)(b, h) = \iota(a)s(g)\iota(b)s(h) = \iota(a + gb)s(g)s(h) = \iota(a + bg + f(g, h))s(gh)$$

Allora la legge di gruppo è data dal prodotto indotto da E, ovvero:

$$(a, g)(b, h) = (a + gb + f(g, h), gh) \tag{5}$$

Abbiamo ora due possibilità: se s è un omomorfismo infatti, la funzione f è costantemente nulla, e la legge di gruppo trovata coincide con la legge di un prodotto semidiretto (in notazione additiva), in caso contrario si vuole capire meglio come classificare le estensioni così trovate. Il primo approccio vedrà l'utilizzo del primo gruppo di coomologia di G a coefficienti in A, mentre la seconda del secondo.

Vediamo nel dettaglio:

7.1. $\mathrm{H}_1(G, A)$**.** Supponiamo che s sia un omomorfismo; la legge di gruppo trovata sopra ci dice che l'unica estensione di G tramite A che induce la stessa azione iniziale, dà luogo al prodotto semidiretto di legge $(a, g)(b, h) = (a + gb, gh)$.

Definizione 24. Diciamo che un ampliamento *spezza* se esiste una sezione $s\colon G \to E$ che è un omomorfismo di gruppi. Chiamiamo in tal caso s *spezzamento* dell'estensione.

Proposizione 25. *Un ampliamento di G tramite il G-modulo A spezza se e solo se è equivalente all'estensione*

$$0 \longrightarrow A \xrightarrow{\iota'} A \rtimes G \xrightarrow{\pi'} G \longrightarrow 1 \tag{6}$$

dove ι' e π' sono le canoniche inclusioni e proiezioni.

Dimostrazione. La successione (6) ammette la sezione $s\colon G \to A \rtimes G$ data da $s(g) = (0, g)$. Inoltre

$$s(g)s(h) = (0, g)(0, h) = (0, gh) = s(gh)$$

cioè s è un omomorfismo. Chiaramente lo stesso vale per una qualsiasi estensione equivalente all'ampliamento (6).

Viceversa, definiamo un omomorfismo $\psi\colon A \rtimes G \to E$ che faccia commutare il diagramma:

$$\begin{tikzcd}
 & & A \rtimes G \arrow[dd, dashed, "\psi"] \arrow[dr, "\pi'"] & & \\
0 \arrow[r] & A \arrow[ur, "\iota'"] \arrow[dr, "\iota"'] & & G \arrow[r] & 1 \\
 & & E' \arrow[ur, "\pi"'] & &
\end{tikzcd}$$

Definiamo $\psi(a, g) = \iota(a)s(g)$; allora ψ è un omomorfismo in quanto

$$\begin{aligned}
\psi((a_1, g_1)(a_2, g_2)) &= \psi(a_1 + g_1 a_2, g_1 g_2) = \iota(a_1)\iota(g_1 a_2)s(g_1 g_2) \\
&= \iota(a_1)s(g_1)\iota(a_2)(s(g_1))^{-1}s(g_1)s(g_2) \\
&= \iota(a_1)s(g_1)\iota(a_2)s(g_2) = \psi(a_1, g_1)\psi(a_2, g_2)
\end{aligned}$$

Inoltre $\pi(\psi(a,g)) = \pi(\iota(a)s(g)) = \pi(\iota(a))\pi(s(g)) = g$ e $\psi(\iota(a) = \psi(a,1) = \iota(a)$, cioè il diagramma commuta e le due estensioni sono equivalenti. $\square$

Abbiamo mostrato che ogni altra estensione per cui esiste un omomorfismo di gruppi s che è una sezione di π è equivalente all'ampliamento (6). È interessante a questo punto capire in che modo, e quanti modi abbiamo di scegliere delle sezioni di G in $A \rtimes G$.

A questo scopo, fissiamo l'estensione (6) che induce l'azione di G su A e una qualunque sezione $s\colon G \to A \rtimes G$. Allora $s(g) = (d(g), g))$, dove $d\colon G \to A$ è un'opportuna funzione che verifica la relazione per ogni $g \in G$.

Svolgendo i prodotti otteniamo:

$$s(g)s(h) = (d(g), g)(d(h), h) = (d(g) + gd(h), gh)s(gh) = (d(gh), gh)$$

Dunque s è un omomorfismo se e solo se

$$d(gh) = d(g) + gd(h)$$

Definizione 26. Una funzione $d\colon G \to A$ per cui

$$d(gh) = d(g) + gd(h)$$

vale per ogni g, $h \in G$, è detta *derivazione*.

Definizione 27. Diciamo che due spezzamenti s_1, s_2 sono A-*coniugati* se esiste un elemento $a \in A$ tale che

$$s_1(g) = \iota(a)s_2(g)(\iota(a))^{-1}$$

per ogni $g \in G$.

La relazione di A-coniugio per due sezioni dell'estensione (6) diventa:

$$\iota(a)s_2(g)(\iota(a))^{-1} = (a,1)(b,g)(a,1)^{-1} = (a+b,g)(a,1)^{-1} = (a+b-ga,g) = s_2(g)$$

ovvero $d_1(g) = a + d_2(g) - ga$, dove d_1 e d_2 sono le derivazioni associate alle due sezioni. Allora d_1, d_2 corrispondono a spezzamenti A-coniugati se e solo se $d_2 - d_1\colon G \to A$ è una funzione della forma $g \mapsto ga - a$ per qualche $a \in A$.

Definizione 28. Una tale derivazione $d\colon G \to A$ è detta *derivazione principale*.

Teorema 29. *Per ogni G-modulo A, le classi di spezzamento A-coniugate dell'estensione*

$$0 \longrightarrow A \xrightarrow{\iota'} A \rtimes G \xrightarrow{\pi'} G \longrightarrow 1$$

sono in corrispondenza biunivoca con $\mathrm{H}^1(G,A)$.

Osservazione 30. Per ogni gruppo G possiamo sempre considerare la *bar-resolution* F. Osserviamo che, in tal caso, posto $C^n(G,M)$ l'n-esimo gruppo di cocatene $\mathrm{Hom}_{\mathbb{Z}G}(F_n, M)$, ogni cocatena $f\colon F_n \to M$ può esser vista come una funzione $F\colon G^n \to M$ data da $F(x,y) = f([x|y])$. La mappa di cobordo $\delta\colon C^{n-1}(G,M) \to C^n(G,M)$ è data allora da:

$$(\delta F)(g_1,\dots,g_n) = F\partial[g_1|\dots|g_n] = g_1F(g_2,\dots,g_n) - F(g_1g_2,\dots,g_n) + \cdots + (-1)^nF(g_1,\dots,g_{n-1})$$

Analogamente, possiamo considerare la risoluzione normalizzata; indichiamo con $C_N^*(G, M)$ il complesso di cocatene costituito dalle mappe F tali che $F(g_1, \ldots, g_n) = 0$ ogni qual volta $g_i = 1$ per qualche indice i.

Dimostrazione. Abbiamo visto che le classi di spezzamento A-coniugate sono proprio le derivazioni quozientate per le derivazioni principali, e per l'osservazione precedente ogni derivazione (principale) si può vedere come cociclo (cobordo). Ora, se P è una risoluzione proiettiva di $\mathbb{Z}$ tramite $\mathbb{Z}G$-moduli, e passando ai duali, abbiamo che

$$\mathrm{H}^1(G, A) \simeq \ker(\delta_1)/\mathrm{Im}(\delta_0)$$

Sia allora $f \in \mathrm{Hom}_G(P_1, A)$;

$$(\delta_1(f))(x, y) = f(\partial[x|y]) = f(x[y] - [xy] + [x]) = xf(y) - f(xy) + f(x)$$

è nullo se e solo se $f(xy) = f(x) + xf(y)$, ovvero se e solo se f è una derivazione.

Infine g è nell'immagine di δ_0 se esiste una mappa $f \colon F_0 \to A$ tale che $g = \delta_0(f)$; ma

$$g(x) = (\delta_0(f))(x) = f(\partial_0[x]) = f(x[\,] - [\,]) = xf(1) - f(1)$$

e quindi g è una derivazione principale. Ciò conclude la dimostrazione del teorema. $\square$

7.2. $\mathrm{H}^2(G, A)$**.** Vediamo infine il caso in cui la sezione normalizzata s non è un omomorfismo e quindi la mappa f in (5) è non banale.

Ricordiamo che esiste una bigezione $\psi \colon A \times G \to E$ definita da $\psi(a, g) = \iota(a)s(g)$, e la legge di gruppo indotta da E:

$$(a, g)(b, h) = (a + gb + f(g, h), gh)$$

Per sottolineare la dipendenza dalla mappa f, denotiamo con E_f il gruppo $A \times G$ con quest'operazione. Osserviamo che E_f risulta essere un'estensione di G equivalente a quella di partenza. Infatti, poiché $\iota(a) = \iota(a)s(1)$ per ogni $a \in A$, la composizione $\iota' \colon A \to E \to E_f$ risulta essere l'inclusione canonica, in quanto $\iota'(a) = \psi^{-1}\iota(a) = \psi^{-1}(\iota(a)s(1)) = (a, 1)$. Analogamente, la composizione $\pi' \colon E_f \to E \to G$ coincide con la proiezione canonica, in quanto $\pi'(a, g) = \pi(\psi(a, g)) = \pi(\iota(a)s(g)) = \pi(s(g)) = g$. Infine queste mappe sono in successione esatta, il diagramma è commutativo, e quindi le due estensioni sono equivalenti:

$$\begin{tikzcd}
 & & E_f \arrow[dd, dashed, "\psi"] \arrow[dr, "\pi'"] & & \\
0 \arrow[r] & A \arrow[ur, "\iota'"] \arrow[dr, "\iota"'] & & G \arrow[r] & 1 \\
 & & E \arrow[ur, "\pi"'] & &
\end{tikzcd}$$

Ciò implica inoltre che entrambe inducono l'azione di G su A fissata, e quindi ad ogni estensione è possibile associare un'estensione equivalente che dipende solo da A, G e dalla funzione f.

Si è appena visto che E_f con l'operazione (5) è un gruppo; in particolare vale la proprietà associativa, e svolgendo i prodotti

$$[(a,g)(b,h)](c,k) = (a+gb+f(g,h),gh)(c,k) = (a+gb+f(g,h)+ghc+f(gh,k),ghk)$$
$$(a,g)[(b,h)(c,k)] = (a,g)(b+hc+f(h,k),hk) = (a+gb+ghc+gf(h,k)+f(g,hk),ghk)$$

otteniamo che f verifica la relazione seguente:

$$gf(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0 \tag{7}$$

Dunque f è per l'osservazione (30) un 2-cociclo, ovvero un elemento di $\ker(\delta_2)$, dove δ_2 è il morfismo di cobordo della successione di cocatene associata alla risoluzione standard di G. Ricordiamo che si era anche richiesta la condizione di normalizzazione di s, da cui abbiamo visto che $f(1,g) = f(g,1) = 0$; detto in altri termini, f si annulla se almeno una variabile è pari a 1, ovvero $f \in C^2_N(G,A)$. Ad ogni estensione di sezione normalizzata abbiamo dunque associato un 2-cociclo normalizzato in $C^2_N(G,A)$.

Viceversa, sia $f \in C^2_N(G,A)$; allora su $A \times G$ possiamo definire il prodotto visto in (5); tale prodotto è sicuramente associativo, in quanto è soddisfatta la condizione di cociclo, e poiché f è normalizzata, si ha l'esistenza di un elemento neutro. Se $(a,g) \in A \times G$ infatti:

$$(a,g)(0,1) = (a+f(g,1),g) = (a,g) \text{ e } (0,1)(a,g) = (a+f(1,g),g) = (a,g).$$

Infine, se $(a,g) \in A \times G$

$$(a,g)(-g^{-1}a - g^{-1}f(g,g^{-1}),g^{-1}) = (a-gg^{-1}a-gg^{-1}f(g,g^{-1})+f(g,g^{-1}),gg^{-1}) = (0,1)$$

e si ha anche l'esistenza di un inverso. Dunque se f è un cociclo normalizzato, $A \times G$ ammette una struttura di gruppo che denoteremo ancora con E_f. Vediamo che esso dà effettivamente un ampliamento di G tramite A con l'azione cercata.

Poniamo $\iota\colon A \to E_f$, $\iota(a) = (a,1)$ e $\pi\colon E_f \to G$, $\pi(a,g) = g$.

- $\iota(a+b) = (a+b,1) = (a+b+f(1,1),1) = (a,1)(b,1) = \iota(a)\iota(b)$, ovvero ι è un omomorfismo;
- $\pi((a,g)(b,h)) = \pi(a+gb+f(g,h),gh) = gh = \pi(g)\pi(h)$, ovvero π è un omomorfismo;
- ι è chiaramente iniettiva, π è surgettiva, e $\pi(\iota(a)) = \pi(a,1) = 1$, ovvero la successione

  $$0 \longrightarrow A \xrightarrow{\ \iota\ } E_f \xrightarrow{\ \pi\ } G \longrightarrow 1$$

  è esatta, ovvero un ampliamento di G tramite A;
- scegliamo come sezione s di π la mappa $g \mapsto s(g) = (0,g)$. L'azione indotta dall'estensione è data da:

  $$\begin{aligned}\iota(ga) = s(g)\iota(a)(s(g))^{-1} &= (0,g)(a,1)(-g^{-1}f(g,g^{-1}),g^{-1})\\ &= (ga+f(g,1),g)(-g^{-1}f(g,g^{-1}),g^{-1})\\ &= (ga-gg^{-1}f(g,g^{-1})+f(g,g^{-1}),gg^{-1}) = (ga,1)\end{aligned}$$

  e quindi l'azione indotta coincide con quella inizialmente fissata su A.
- infine mostriamo che la funzione che corrisponde alla sezione s scelta è proprio la mappa f; ma infatti

  $$s(g)s(h) = (0,g)(0,h) = (f(g,h),gh) = (f(g,h),1)(0,gh) = \iota(f(g,h))s(gh).$$

Ciò dimostra allora che la corrispondenza tra estensioni con sezione normalizzata e 2 cocicli normalizzati in $C^*_N(G, A)$ è biunivoca.

Concludiamo con il risultato di classificazione delle estensioni:

Teorema 31. *Sia A un G-modulo e sia $\mathcal{E}(G, A)$ l'insieme delle classi di equivalenza di estensioni di G tramite A che danno luogo alla fissata azione di G su A. Allora esiste una bigezione*

$$\mathcal{E}(G, A) \simeq \mathrm{H}^2(G, A).$$

Dimostrazione. Vediamo cosa succede cambiando la scelta della sezione s di π. Poiché s dà un insieme di rappresentanti dei coset di $\iota(A)$ in G, una qualunque altra sezione normalizzata t differisce da s per un elemento di $\iota(A)$, ovvero esiste una mappa $c\colon G \to A$ tale che

$$t\colon g \mapsto t(g) = \iota(c(g))s(g) \quad \forall g \in G.$$

Inoltre tale mappe è tale che $c(1) = 0$, quindi c si può vedere come un elemento arbitrario di $C^1_N(G, A)$.

Calcoliamo il 2-cociclo corrispondente a questa nuova sezione:

$$\begin{aligned} t(g)t(h) = \iota(c(g))s(g)\iota(c(h))s(h) &= \iota(c(g))\iota(gc(h))s(g)s(h) \\ &= \iota(c(g) + gc(h))\iota(f(g, h))s(gh) \\ &= \iota(c(g) + gc(h) + f(g, h))s(gh) \\ &= \iota(c(g) + gc(h) + f(g, h) - c(gh))\iota(c(gh))s(gh) \\ &= \iota(c(g) + gc(h) + f(g, h) - c(gh))t(gh) \end{aligned}$$

La mappa $f'\colon G \times G \to A$ associa allora ad ogni coppia $(g, h) \in G \times G$ l'elemento

$$c(g) + gc(h) + f(g, h) - c(gh).$$

Ma $\delta_1(c)$ è esattamente $gc(h) - c(gh) + c(g)$, ovvero

$$f' = f + \delta_1(c)$$

e quindi la scelta di una diversa sezione normalizzata corrisponde esattamente a modificare il cociclo normalizzato f per un cobordo.

Consideriamo ora due estensioni equivalenti:

$$\begin{tikzcd} & & E \arrow[dd, dashed, "\psi"] \arrow[dr, "\pi"] & & \\ 0 \arrow[r] & A \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & & G \arrow[r] & 1 \\ & & E' \arrow[ur, "\pi'"'] & & \end{tikzcd}$$

scegliamo una sezione normalizzata s di π ed s' di π'; a queste corrispondono due 2-cocicli f ed f', tali che $s(g)s(h) = \iota(f(g, h))(s(gh))$ ed $s'(g)s'(h) = \iota'(f'(g, h))(s'(gh))$. La composizione $\psi^{-1}s'$ è un'altra sezione normalizzata di π, e dunque i cocicli f e il nuovo 2-cociclo relativo alla sezione $\psi^{-1}s'$, per quanto appena dimostrato, differiscono per un cobordo. Ma vediamo che questo cociclo non è altri che f'; e infatti

$$\psi^{-1}(s'(g))\psi^{-1}(s'(h)) = \psi^{-1}(s'(g)s'(h)) = \psi^{-1}(\iota'(f'(g,h))s'(gh)) = \iota(f'(g,h))\psi^{-1}(s'(gh))$$

Ciò dimostra che, date due estensioni equivalenti di G tramite A, i 2-cocicli corrispondenti differiscono sempre per un cobordo, e quindi determinano un unico elemento in $\mathrm{H}^2(G,A)$.

Viceversa, supponiamo di avere due elementi f, f' in $C^2_N(G,A)$ che differiscono per un cobordo, diciamo $f' = f + \delta_1(c)$. Sia $\phi\colon E_{f'} \to E_f$ definita da $\phi(a,g) = (a+c(g),g)$. Questo è un omomorfismo di gruppi, in quanto:

$$\begin{aligned}
\phi(a,g)\phi(b,h) &= (a+c(g),g)(b+c(h),h)\\
&= (a+c(g)+gb+gc(h)+f(g,h),gh)\\
&= (a+gb+f'(g,h)-f(g,h)+c(gh)+f(g,h),gh)\\
&= \phi(a+gb+f'(g,h),gh) = \phi((a,g)(b,h))
\end{aligned}$$

Inoltre il diagramma

$$\begin{tikzcd}
 & & E_{f'} \arrow[dd, dashed, "\phi"] \arrow[dr, "\pi'"] & & \\
0 \arrow[r] & A \arrow[ur, "\iota'"] \arrow[dr, "\iota"'] & & G \arrow[r] & 1 \\
 & & E_f \arrow[ur, "\pi"'] & &
\end{tikzcd}$$

è commutativo in quanto $\phi(\iota'(a)) = \phi(a,1) = (a+c(1),1) = (a,1) = \iota(a)$ e in modo analogo $\pi'(\phi(a,g)) = \pi'(a+c(g),g) = g = \pi(a,g)$. Ciò vuol dire che a cocicli che differiscono per un cobordo corrispondono estensioni equivalenti. Ciò conclude la dimostrazione. $\square$