Università degli Studi di Pisa

FACOLTÀ DI MATEMATICA
Corso di Laurea triennale in Matematica

Tesi di laurea triennale

Hopf-algebre e teoria di Galois

Candidato:
Davide Lofano

Relatrice:
Ilaria Del Corso

Anno Accademico 2015–2016

Indice

Introduzione

A partire dagli anni 60 ma con maggior frequenza verso la fine degli anni 80 le Hopf-algebre hanno iniziato a comparire nella teoria algebrica dei numeri in relazione alle estensioni intere. Il problema è quello di classificare le estensione che ammettono una base normale intera su un modulo opportuno. Con questo scopo è stata introdotta la definizione di estensioni Hopf-Galois che ha permesso di giungere ad una generalizzazione del teorema di Noether. Noi tuttavia non ci soffermeremo su tale generalizzazione, scopo della tesi sarà invece presentare le Hopf-algebre e, concentrandoci sulle estensioni separabili, provare a classificare le strutture Hopf-Galois qui presenti.

Nel primo capitolo vengono presentate le Hopf-algebre, degli spazi vettoriali dotati sia di una struttura di algebra che di coalgebra e dove le due strutture sono compatibili tra loro. Verrà presentato l'esempio più importante di Hopf-algebra, ovvero le algebre di gruppo, e verrannno dimostrate le principali proprietà di tali strutture che serviranno nelle dimostrazioni successive. In particolare ci soffermeremo sulla definizione di Hopf-algebra duale e sulla sua correlazione con la Hopf-algebra di partenza, strumento indispensabile per la dimostrazione del teorema principale che affronteremo nel terzo capitolo. Verranno inoltre introdotte ulteriori definizioni, in particolare quella di modulo algebra, un modulo con delle ulteriori proprietà e la sua definizione duale ovvero quella di comodulo algebra.

Nel secondo capitolo, dopo un breve ripasso di teoria di Galois classica, viene invece introdotta la definizione di estensione Hopf-Galois:

Definizione 0.0.1. Sia L/k un'estensione finita di campi ed H una $k-$Hopf-algebra. L si dice una *estensione* $H-Galois$ se L è una $H-$modulo algebra e il morfismo di moduli $j : L \otimes H \to End_k(L)$ definito come

$$j(l \otimes h)(t) = lh(t)$$

è in realtà un isomorfismo di algebre.

Successivamente viene fatto notare che le estensioni di Galois classiche sono anche estensioni Hopf-Galois e quindi che quella presentata è effettivamente una generalizzazione della teoria standard. Vengono infine presentati e parzialmente

dimostrati alcuni lemmi tecnici. In particolare si vede come la definizione precedente può essere scritta anche facendo uso dell'Hopf-algebra duale ottenendo una struttura che viene chiamata oggetto di Galois. Viene anche introdotta la teoria di Morita, uno strumento fondamentale per le dimostrazioni successive, la quale studia la relazione tra le categorie dei $k-$moduli e quella degli $End_k(A)-$moduli dove A è un $k-$modulo.

Il capitolo successivo è interamente dedicato alla dimostrazione di un teorema dovuto a Greither e Pareigis il quale permette di conoscere tutte le diverse strutture Hopf-Galois di una certa estensione separabile.

Teorema 0.0.2. *Sia L/k un'estensione finita e separabile di campi con chiusura normale E e sia $G = Gal(E/k)$, $G' = Gal(E/L)$, $X = G/G'$. Esiste allora una bigezione tra i sottogruppi regolari N di $Perm(X)$ normalizzati da $\lambda(G)$ e le Hopf-Galois strutture su L/k.*

Dove $\lambda(G)$ è l'ovvia immersione di G in $Perm(X)$. La dimostrazione come detto è alquanto lunga e laboriosa, ma l'idea principale è quella di considerare l'estensione $E \otimes L$ (usando le notazione di sopra). Tale estensione risulterà essere isomorfa a XE, dove con questa notazione intendiamo le mappe che vanno da X in E. Si vedrà che su tali estensioni le strutture Hopf-Galois si riescono a calcolare molto più facilmente. A questo punto, utilizzando, come già anticipato, la teoria di Morita si riesce a tornare all'estensione di partenza.

Nel quarto capitolo vengono invece presentati vari esempi e corollari di utilizzo del teorema. Si vedrà in particolare che per prima cosa non è detto che tutte le estensioni separabili ammettano una struttura Hopf-Galois e viceversa che se ne ammettono una non è detto che essa sia unica. Verrà studiato esplicitamente il caso delle estensioni di Galois classiche nelle quali si faranno vedere due strutture diverse se il gruppo di Galois è non abeliano, con il calcolo esplicito delle strutture nel caso di S_3. Si dimostrerà inoltre che tutte le estensioni di grado quattro o inferiore ammettono almeno una struttura Hopf-Galois mentre si farà vedere un esempio di estensione di quinto grado che non ne ammette nessuna. Si concluderà calcolando esplicitamente le Hopf-algebre relative ad una certa estensione di $\mathbb{Q}$ di quarto grado che ammette due strutture Hopf-Galois distinte.

Nell'ultimo capitolo infine vengono presentati vari teoremi, in gran parte non dimostrati nella tesi, con lo scopo di dare una panoramica su quanto è stato finora detto su tali estensioni. In particolare ci soffermeremo sul lavoro di Byott che è riuscito a riformulare il teorema di Greither e Pareigis in una forma più semplice invertendo in un certo senso la relazione i gruppi G e $Perm(X)$. In questo modo si è riusciti a dimostrare che un'estensione separabile di grado primo è Hopf-Galois se e solo se il gruppo di Galois della sua chiusura normale è risolubile ed anche che un'estensione di Galois classica ammette un'unica struttura Hopf-Galois se e solo se il grado della sua estensione è coprimo con la sua ϕ di Eulero. Vedremo inoltre

nell'ultima parte come si riesce a generalizzare in maniera parziale il teorema di corrispondenza di Galois classico, in particolare una delle due frecce del teorema, ovvero l'iniettività, è vera sempre, l'altra invece solo in alcuni casi particolari che verranno per questo motivo chiamate estensione di Galois quasi classiche.

Capitolo 1

Hopf-algebre e loro proprietà

In questo primo capitolo partiremo dalle definizioni di algebra e coalgebra per poi arrivare alla definizione di Hopf-algebra e dimostreremo le pricipali proprietà di tali strutture che verranno usate nei successivi capitoli. Il riferimento principale saranno le prime novanta pagine del testo di Sweedler [1].

1.1 Algebre e coalgebre

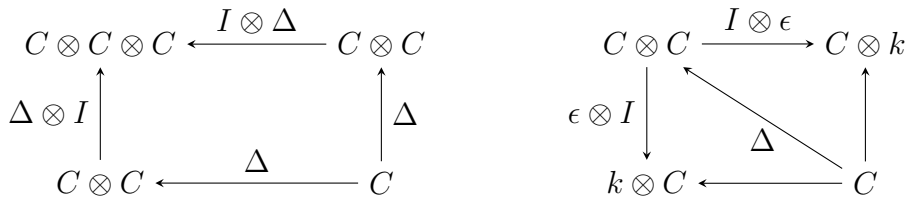
Definizione 1.1.1. Sia k un campo, un'*algebra* su k è una tripla (A, M, u) dove A è un $k-$spazio vettoriale, M una mappa $k-$lineare chiamata moltiplicazione da $A \otimes A$ in A e u una mappa $k-$lineare chiamata la mappa unità da k in A tali che i due seguenti diagrammi siano commutativi:

$$\begin{array}{ccc} A\otimes A\otimes A & \xrightarrow{I\otimes M} & A\otimes A \\ {\scriptstyle M\otimes I}\downarrow & & \downarrow{\scriptstyle M} \\ A\otimes A & \xrightarrow{M} & A \end{array} \qquad \begin{array}{ccc} A\otimes A & \xleftarrow{I\otimes u} & A\otimes k \\ {\scriptstyle u\otimes I}\uparrow & \nearrow_{M} & \downarrow \\ k\otimes A & \longrightarrow & A \end{array}$$

Dove la mappa I è la mappa identità e, dove non sono specificate, le mappe sono le immersioni ovvie.

Si può notare facilmente che tale definizione coincide con quella più elementare data usualmente, ma la comodità di questo approccio è che ci permette di definire immediatamente la struttura di coalgebra semplicemente girando le frecce nei diagrammi precedenti, abbiamo quindi la seguente definizione:

Definizione 1.1.2. Sia k un campo, una *coalgebra* è una tripla (C, Δ, ϵ) dove C è un $k-$spazio-vettoriale, Δ una mappa $k-$linearer chiamata comoltiplicazione da C in $C \otimes C$ e ϵ una mappa $k-$lineare chiamata counità da C in k, tali che i seguenti diagrammi siano commutativi:



Nel seguito, laddove le mappe saranno chiare, identificheremo un'algebra o una coalgebra semplicemente con lo spazio vettoriale. Inoltre, laddove non ci posso essere confusione, scriveremo la moltiplicazione nella maniera usuale, ovvero dato $a, b \in A$ algebra indicheremo con ab l'elemento $M(a \otimes b)$.

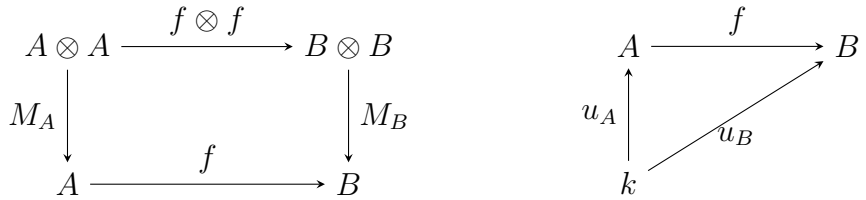
Nota 1.1.3. Data una coalgebra come nella definizione introdurremo la notazione: $\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$, dove $c_{(1)}$ e $c_{(2)}$ sono elementi di C.

Esempio 1.1.4. Un facile esempio di coalgebra, che verrà approfondito successivamente, è il seguente: sia S un insieme, denoto con kS lo spazio vettoriale su k che ha S come base. Definisco $\Delta(s) = s \otimes s, \epsilon(s) = 1 \ \forall s \in S$, estendo tali mappe su tutto kS ed ottengo una struttura di coalgebra.

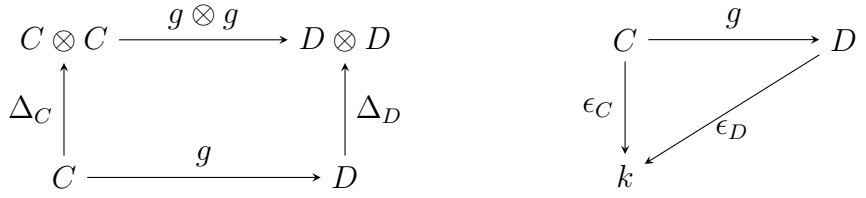
Definizione 1.1.5. Sia C una coalgebra, gli elementi $c \in C$ tali che $\Delta(c) = c \otimes c$ sono chiamati *elementi group-like*.

Avendo definito gli oggetti su cui vogliamo lavorare, bisogna ora definire le mappe tra tali oggetti.

Definizione 1.1.6. Siano A e B due algebre, una mappa lineare $f : A \to B$ si dice *morfismo di algebre* se i seguenti diagrammi sono commutativi:



Definizione 1.1.7. Siano C e D due coalgebre, una mappa lineare $g : C \to D$ si dice *morfismo di coalgebre* se i seguenti diagrammi sono commutativi:



Definizione 1.1.8. Sia (C, Δ, ϵ) una coalgebra e sia V uno sottospazio vettoriale tale che $\Delta(V) \subseteq V \otimes V$. Allora $(V, \Delta|_V, \epsilon|_V)$ è una coalgebra e si chiama *sottocoalgebra* di C. Inoltre la mappa di inclusione è un morfismo di coalgebre.

Prendiamo ora uno spazio vettoriale V su k, ricordiamo che il suo spazio duale è lo spazio degli omomorfismi $k-$lineari da V a k che denotiamo con V^*. Inoltre una mappa $L : V \to W$ induce in maniera canonica una mappa $L^* : W^* \to V^*$ dove dato $f \in W^*$ e $v \in V$ ho che $L^*(f)(v) = f(L(v))$. Data allora una coalgebra (C, Δ, ϵ) avrò due mappe $\Delta^* : (C \otimes C)^* \to C^*$ e $\epsilon^* : k^* \to C^*$. Inoltre $C^* \otimes C^*$ si immerge naturalmente in $(C \otimes C)^*$ tramite l'omomorfismo ρ che manda $(f \otimes g)(v \otimes w)$ in $f(v)g(w)$. Mentre k^* è isomorfo in maniera naturale a k, posso quindi definire a partire da Δ^* e ϵ^* due mappe $M : C^* \otimes C^* \to C^*$ e $u : k \to C^*$ e vale che:

Proposizione 1.1.9. *Nelle notazioni precedenti (C^*, M, u) è un'algebra*

Dimostrazione. Voglio scrivermi in maniera esplicita le mappe M e u. Siano quindi c^* e d^* due elementi di C^* e $h \in C$, per quanto detto sopra abbiamo che $M(c^* \otimes d^*)(h) = \Delta^* \circ \rho(c^* \otimes d^*)(h) = \rho(c^* \otimes d^*)(\Delta(h)) = \sum_{(h)} c^*(h_{(1)})d^*(h_{(2)})$. Mentre $u(1_k(h)) = \epsilon(h)$. Avendo scritto espressamente le mappe la verifica che C^* è un'algebra a questo punto è un semplice conto un po' lungo di cui trascuriamo i dettagli.

□

Inoltre vale anche il duale di tale proposizione, ma solo se l'algebra di partenza A ha dimensione finita, in tal caso infatti l'immersione da $A^* \otimes A^*$ in $(A \otimes A)^*$ è in realtà un isomorfismo. Operando nello stesso modo riesco quindi, a partire dalle mappe che mi definiscono l'algebra, a costruire due mappe che mi definiscono la coalgebra A^*. In particolare le mappe Δ e ϵ saranno definite come: $\Delta(a^*)(h \otimes j) = a^*(M(h \otimes j))$ e $\epsilon(a^*) = a^*(u(1))$.

Se H è una spazio vettoriale finitamente generato sappiamo che esso è canonicamente isomorfo a H^{**} tramite l'isomorfismo ϕ tale che $\phi(a) = f_a$ dove $f_a(g) = g(a)$. Tale isomorfismo può essere esteso alle algebre e alle coalgebre.

Proposizione 1.1.10. *Se H è un'algebra (risp. una coalgebra) finitamente generata, allora è isomorfa come algebra (risp. coalgebra) a H^{**}.*

Dimostrazione. Dimostrerò la proposizione solo nel caso in cui H sia una coalgebra ma nell'altro caso la dimostrazione è del tutto equivalente. Per prima cosa scriviamo quali sono le mappe di H^{**} che chiameremo Δ^{**} e ϵ^{**}. Sia $f_a \in H^{**}$ e $g, h \in H^*$, dove f_a è ottenuto da $a \in H$ tramite l'isomorfismo ϕ. $\Delta^{**}(f_a)(g \otimes h) = f_a(M^*(g \otimes h)) = M^*(g \otimes h)(a) = \sum_{(a)} g(a_{(1)})h(a_{(2)})$ dove ovviamente M^* è la moltiplicazione in H^* mentre $\epsilon^{**}(f_a) = f_a(u^*(1)) = (u^*(1))(a) = \epsilon(a)$. La commutatività del secondo diagramma è quindi ovvia, verifichiamo quella del primo. Sia

$a \otimes b \in H \otimes H$, $(\phi \otimes \phi)(a \otimes b) = f_a \otimes f_b$. Sia allora $h \in H$ e $g, k \in H^*$:

$$\Delta^{**} \circ \phi(h)(g \otimes k) = \Delta^{**}(f_h)(g \otimes k) = \sum_{(h)} g(h_{(1)})k(h_{(2)})$$

$$(\phi \otimes \phi) \circ \Delta(h)(g \otimes k) = (\phi \otimes \phi)(\sum_{(h)} h_{(1)} \otimes h_{(2)})(g \otimes k) = (\sum_{(h)} f_{h_{(1)}} \otimes f_{h_{(2)}})(g \otimes k)$$

e le due espressioni sono equivalenti. □

Un altro concetto che ci tornerà molto utile è quello della commutatività e cocommutatività.

Definizione 1.1.11. Un'algebra A si dice *commutativa* se $M(a \otimes b) = M(b \otimes a)$.
Una coalgebra C si dice *cocommutativa* se $\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)} = \sum_{(c)} c_{(2)} \otimes c_{(1)}$.

Per come abbiamo definito le mappe che mandano una coalgebra nella sua algebra duale segue immediatamente che una coalgebra è cocommutativa se e solo se la sua algebra duale è commutativa e viceversa. Vale inoltre, per la linearità di Δ che se una coalgebra è Span di elementi cocommutativi allora sarà cocommutativa. Quindi la coalgebra dell'1.1.4 è cocommutativa.

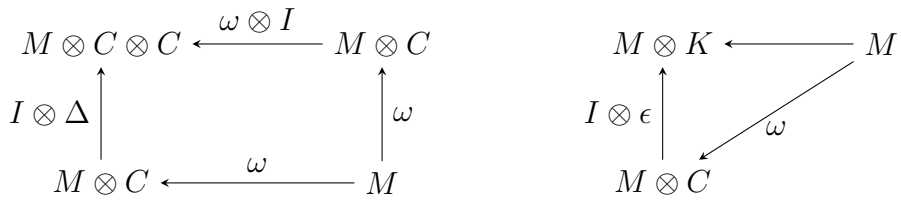
1.2 Moduli e comoduli

Seguendo lo stesso approccio della sezione precedente ridefiniremo la nozione di modulo utilizzando il prodotto tensore in modo che la definizione di comodulo seguirà spontaneamente.

Definizione 1.2.1. Se A è un'algebra un $A-$*modulo sinistro* è uno spazio vettoriale N dotato di una mappa $\psi : A \otimes N \to N$ che rende i due seguenti diagrammi commutativi:

$$\begin{array}{ccc} A \otimes A \otimes N & \xrightarrow{I \otimes \psi} & A \otimes N \\ \downarrow{\scriptstyle M \otimes I} & & \downarrow{\scriptstyle \psi} \\ A \otimes N & \xrightarrow{\psi} & N \end{array} \qquad \begin{array}{ccc} k \otimes N & \longrightarrow & N \\ \downarrow{\scriptstyle u \otimes I} & \nearrow{\scriptstyle \psi} & \\ A \otimes N & & \end{array}$$

Definizione 1.2.2. Se C è una coalgebra un $C-$*comodulo destro* è uno spazio vettoriale M dotato di una mappa $\omega : M \to M \otimes C$ che rende i due seguenti diagrammi commutativi:



Nota 1.2.3. Come avevamo fatto nel caso delle coalgebre scriveremo che $\omega(m) = \sum_{(m)} m_{(0)} \otimes m_{(1)}$ dove $m_{(0)} \in M$ e $m_{(1)} \in C$.

Sempre dualizzando, ed avendo in mente cosa è un morfismo di moduli, otteniamo che se M e N sono due comoduli destri una mappa $f : M \to N$ è un morfismo di comoduli se commuta il seguente diagramma:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \omega_M}\downarrow & & \downarrow{\scriptstyle \omega_N} \\ M \otimes C & \xrightarrow{f \otimes I} & N \otimes C \end{array}$$

Inoltre, definendo un sottocomodulo come avevamo definito una sottocoalgebra ovvero un sottospazio vettoriale N tale che $\psi(N) \subseteq N \otimes C$, abbiamo che i comoduli ereditano la maggior parte delle proprietà dei moduli. In particolare se ho un morfismo di comoduli allora il Ker e l'immagine saranno due sottocomoduli e valgono anche i teoremi di omomorfismo.

Avendo parlato nella sezione precedente di algebre e coalgebre duali viene naturale chiedersi quale sia la relazione tra i comoduli di una coalgebra e i moduli dell'algebra duale e viceversa. Sia quindi C una coalgebra e C^* la sua algebra duale. Data una mappa lineare $\omega : M \to M \otimes C$ riusciamo a costruire una mappa $\psi_\omega : C^* \otimes M \to M$. Per prima cosa notiamo che riusciamo a costruire facilmente una mappa da $C^* \otimes M \otimes C$ in M che chiameremo h. Infatti come primo passo scambiamo gli ultimi due spazi tramite la mappa T che mi manda $c^* \otimes m$ in $m \otimes c^*$. Siamo ora quindi in $M \otimes C^* \otimes C$ agiamo tramite la valutazione sugli ultimi due fattori del prodotto tensore andando quindi in $M \otimes k$ che tramite l'omomorfismo canonico va in M. ψ_ω sarà quindi semplicemente la mappa $h \circ (I \otimes \omega)$.

Proposizione 1.2.4. *(M, ω) è un $C-$comodulo destro se e solo se (M, ψ_ω) è un C^*-modulo sinistro.*

Dimostrazione. Dimostriamo la prima implicazione. Sia quindi M un $C-$comodulo destro, e dato $m \in M$ scrivo $\omega(m)$ come $\sum_{(m)} m_{(0)} \otimes m_{(1)}$ dove la prima componente sta in M e la seconda in C. Mi ricordo che, per come ho definito l'algebra duale, vale che $\epsilon = u(1)$. Per verificare la commutatività del secondo diagramma basta quindi vedere per linearità che $\psi_\omega(\epsilon \otimes m) = m$ per ogni $m \in M$.

$$\psi_\omega(\epsilon \otimes m) = h(\sum_{(m)} \epsilon \otimes m_{(0)} \otimes m_{(1)}) = \sum_{(m)} m_{(0)} \otimes \epsilon(m_{(1)}) = m$$

Dove l'ultima uguaglianza deriva immediatamente dalla definizione di comodulo. Resta quindi da verificare il primo diagramma, cioè che, dati $a^*, b^* \in C^*$ e $m \in M$ vale

$$\psi_\omega \circ (I \otimes \psi_\omega)(a^* \otimes b^* \otimes m) = \psi_\omega \circ (M \otimes I)(a^* \otimes b^* \otimes m)$$

$$\psi_\omega \circ (M \otimes I)(a^* \otimes b^* \otimes m) = \psi_\omega(a^* b^* \otimes m) = \sum_{(m)} m_{(0)}(a^* b^*)(m_{(1)}) =$$
$$= \sum_{(m)} m_{(0)} a^*(m_{(1)}) b^*(m_{(2)})$$

dove l'ultima ugugaglianza vale per come è definita M a partire da Δ cioè $M(c^* \otimes d^*)(h) = \sum_{(c)} c^*(c_{(1)}) d^*(c_{(2)})$ Ricordiamo ora che M è un comodulo, in particolare sappiamo che $\sum_{(m)} m_{(0)} \otimes m_{(1)} \otimes m_{(2)} = (I \otimes \Delta) \circ \omega(m)$ per costruzione. Ma allora sarà anche uguale a $(\omega \otimes I) \circ \omega(m)$. Quindi l'ultima equazione diventa uguale a: $\sum_{(m)} \psi_\omega(a^* \otimes m_{(0)} b^*(m_{(1)})) = \psi_\omega \circ (I \otimes \psi_\omega)(a^* \otimes b^* \otimes m)$.

Quindi M è un C^*-modulo. L'implicazione inversa si risolve in modo simile. □

Corollario 1.2.5. *Sia A un'algebra finitamente generata, allora M è un $A-$modulo sinistro se e solo se è un A^*-comodulo destro.*

Dimostrazione. Deriva immediatamente dalla proposizione precedente e dalla proposizione 1.1.10. □

1.3 Bialgebre

Se A e B sono due algebre è chiaro che posso dotare $A \otimes B$ in maniera canonica di una struttura di algebra. Questo vale anche nel caso di due coalgebre C e D, basta infatti definire $\epsilon_{C\otimes D}(c \otimes d) = \epsilon_C(c)\epsilon_D(d)$ e $\Delta_{C\otimes D}(c \otimes d) = \sum_{(c),(d)} c_{(1)} \otimes d_{(1)} \otimes c_{(2)} \otimes d_{(2)}$ che è semplicemente la definizione duale a quella di prodotto tensore di due algebre.

Sia allora (H, M, u) una algebra e (H, Δ, ϵ) una coalgebra. Per quanto appena detto $H \otimes H$ può essere dotata sia di una struttura di algebra che di coalgebra.

Proposizione 1.3.1. *Nelle notazioni precedenti i seguenti fatti sono equivalenti:*

- *M e u sono morfismi di coalgebre;*
- *Δ e ϵ sono morfismi di algebre.*

Dimostrazione. Per dimostrare l'equivalenza consideriamo i seguenti quattro diagrammi:

$$\begin{array}{ccccc} H\otimes H & \xrightarrow{M} & H & \xrightarrow{\Delta} & H\otimes H \\ {\scriptstyle \Delta\otimes\Delta}\downarrow & & & & \uparrow{\scriptstyle M\otimes M} \\ H\otimes H\otimes H\otimes H & & \xrightarrow{I\otimes T\otimes I} & & H\otimes H\otimes H\otimes H \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\Delta} & H\otimes H \\ {\scriptstyle u}\uparrow & & \uparrow{\scriptstyle u\otimes u} \\ k & \longrightarrow & k\otimes k \end{array}$$

$$\begin{array}{ccc} H\otimes H & \xrightarrow{\epsilon\otimes\epsilon} & k\otimes k \\ {\scriptstyle M}\downarrow & & \downarrow \\ H & \xrightarrow{\epsilon} & k \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\epsilon} & k \\ {\scriptstyle u}\uparrow & \nearrow_{I} & \\ k & & \end{array}$$

La commutatività dei primi due diagrammi dice esattamente che Δ è un morfismo di algebre mentre la commutatività degli ultimi due mi dice che ϵ è un morfismo di algebre. Ma al tempo stesso la commutatività del primo e del terzo mi dice che M è un morfismo di coalgebre mentre quella del secondo e del quarto che u è un morfismo di coalgebre. Quindi è chiaro che le due affermazioni precedenti sono equivalenti. □

Definizione 1.3.2. Sia H uno spazio vettoriale che verifica le condizioni della proposizione precedente, H viene allora chiamata *bialgebra*.

Nota 1.3.3. In alcuni testi H è chiamata Hopf-algebra, noi tuttavia riserveremo questo termine a particolari bialgebre che hanno un'ulteriore proprietà come vedremo nella prossima sezione.

Osservazione 1.3.4. *Dalla proposizione 1.1.9 e dal suo viceversa segue facilmente che se H è una bialgebra finito dimensionale allora anche H^* è una bialgebra.*

Definizione 1.3.5. Se A è un sottospazio di una bialgebra H allora A è una *sottobialgebra* di H se è simultaneamente una sottoalgebra e una sottocoalgebra di H.

Una mappa lineare tra bialgebre è detto *morfismo di bialgebre* se è simultaneamente un morfismo di algebre e un morfismo di coalgebre.

Diamo ora un paio di esempi di bialgebre.

Esempio 1.3.6. Il campo k è una bialgebra con la struttura banale $M = u = \Delta = \epsilon = I$ dove I è la mappa identità.

Esempio 1.3.7. Se G è un gruppo sia kG l'algebra di gruppo. Come nell'esempio 1.1.4 posso dotare kG di una struttura di coalgebra definendo $\Delta(g) = g \otimes g$ e $\epsilon(g) = 1$ per ogni elemente $g \in G$. Vediamo che Δ e ϵ sono morfismi di algebre.

Lo verifichiamo solo per Δ in quanto per ϵ la verifica è banale. Devo vedere che i due diagrammi sono commutativi: partiamo dal secondo cioè devo verificare che $\Delta \circ u_{kG} = u_{kG\otimes kG}$ ma questo è ovvio, infatti dato $x \in k$ $\Delta \circ u_{kG}(x) = \Delta(xI) = x(I \otimes I) = u_{kG\otimes kG}(x)$. Per quanto riguarda il primo diagramma invece noto subito che, essendo tutte le mappe lineari, posso limitarmi a verificare la relazione $M_{kG\otimes kG} \circ (\Delta \otimes \Delta) = \Delta \circ M_{kG}$ solo sugli elementi della forma $g \otimes h$ con $g, h \in G$. Ma allora:

$$M_{kG\otimes kG} \circ (\Delta \otimes \Delta)(g \otimes h) = M_{kG\otimes kG}(g \otimes g \otimes h \otimes h) = gh \otimes gh$$
$$\Delta \circ M_{kG}(g \otimes h) = \Delta(gh) = gh \otimes gh$$

Possiamo quindi concludere che kG è una bialgebra.

1.4 Hopf-algebre

Se C è una coalgebra e A un'algebra possiamo dare a $Hom(C, A)$ una struttura di algebra. Dati $f, g \in Hom(C, A)$ denotiamo con $fg = M_{Hom(C,A)}(f \otimes g)$, basta allora definire $fg(c) = \sum_{(c)} f(c_{(1)})g(c_{(2)})$, tale mappa è usualemtente chiamata convoluzione. Per quanto riguarda la mappa unità invece, dato $c \in C$ e $x \in k$ la definiremo come $u_O(x)(c) = \epsilon(c)u(x)$, dove le mappe sono quelle di C e A. Si può verificare che con questa struttura $Hom(C, A)$ è un'algebra.

Supponiamo ora che H sia una bialgebra. Se chiamiamo con H^C la sua struttura di coalgebra e con H^A la sua struttura di algebra abbiamo che $Hom(H^C, H^A)$ è un'algebra. Sia I la mappa identità da H in H. Notiamo che essa non è l'unità della nostra algebra la quale infatti è l'elemento $u(1)\epsilon$.

Definizione 1.4.1. Un elemento $S \in Hom(H^C, H^A)$ che è inverso tramite a I è chiamato *antipode* per H. Cioè S è un antipode se e solo se $SI = IS = u(1)\epsilon$.

Osserviamo immediatamente che se H ha un antipode allora esso è unico dato che deve essere un inverso sia destro che sinistro di I.

Definizione 1.4.2. Una bialgebra H che ha un antipode è chiamata Hopf-algebra.

Enunciamo ora senza dimostrare una proposizione che descrive le principali proprietà della mappa antipodale, le quali tuttavia non ci serviranno nei capitoli successivi.

Proposizione 1.4.3. *Sia H una Hopf-algebra con antipode S e siano $g, h \in H$ allora:*

- $S(gh) = S(g)S(h)$;

- $S(1) = 1$;
- $\epsilon \circ S = \epsilon$;
- *Se H è commutativa o cocommutativa allora $S \circ S = I$.*

Definizione 1.4.4. Siano H, L due Hopf-algebre con antipodi S_H e S_L, una mappa $f : H \to L$ è detta essere un *morfismo di Hopf-algebre* se è un morfismo di bialgebre e vale che: $S_L \circ f = f \circ S_H$.

Tuttavia si può verificare che la seconda condizione è sempre soddisfatta, ovvero che se H e L sono Hopf-algebre, allora tutti i morfismi di bialgebre sono anche morfismi di Hopf-algebre.

Analogamente definiamo una sottoHopf-algebra come una sottobialgebra che sia anche chiusa rispetto all'antipode.

Osservazione 1.4.5. *Partendo dall'osservazione 1.3.4 se H è una Hopf-algebra allora anche H^* è tale, dove la mappa antipodale sarà data da: $S^*(f)(h) = f(S(h))$ dove $f \in H^*, h \in H$.*

Esempio 1.4.6. Riprendendo l'esempio 1.3.7 riusciamo a dotare kG di una struttura di Hopf-algebra dove la mappa antipodale S è semplicemente definita come l'inverso sugli elementi del gruppo G. Infatti sia $g \in G$ allora $(IS)(g) = gg^{-1} = Id = u(1) = u(1)\epsilon(g)$, similmente si verifica per SI e per linearità si estende su tutto kG.

Nel caso in cui H sia una Hopf-algebra (in realtà è sufficiente una bialgebra) possiamo considerare una classe particolare di moduli. Notiamo infatti che in questo caso se R è un $H-$modulo ed una $k-$algebra possiamo dotare di una struttura di $H-$modulo anche $R \otimes R$ attraverso la mappa Δ_H e k attraverso ϵ.

Definizione 1.4.7. Sia H una Hopf-algebra e sia R una $k-$algebra ed un $H-$modulo. R è una *$H-$modulo algebra* se le mappe M_R e u_R che definiscono la sua struttura come algebra sono morfismi di $H-$moduli.

La definizione precedente implica che $h(st) = \sum_{(h)} h_{(1)}(s)h_{(2)}(t)$ e $h(1) = \epsilon(h)1$ per ogni $h \in H$ e $s, t \in R$.

Esempio 1.4.8. Se L/k è un'estensione di Galois e G è il gruppo di Galois dell'estensione allora L è una $kG-$modulo algebra sinistra. Dove definiamo la mappa ψ che genera la struttura di modulo sugli elementi di G nel modo ovvio e la estendiamo per linearità. Che tale mappa renda L un modulo è ovvio quindi verifichiamo solo la condizione sul fatto che sia una $kG-$modulo algebra, ed ovviamente basta guardare solo sugli elementi di g. Sia quindi $g \in G$ e $s, t \in L$ ma allora $g(st) = g(s)g(t)$ e $g(1) = 1$ quindi entrambe le condizioni sono verificate.

Ovviamente si può parlare anche di $H-$comodulo algebre, dove vediamo k come un $H-$comodulo destro tramite $\alpha(k) = k \otimes 1_H$ mentre in $R \otimes R$ definiamo la mappa che genera la struttura di comodulo come $\beta(s \otimes t) = \sum_{(s),(t)} s_{(0)} \otimes t_{(0)} \otimes M_H(s_{(1)} \otimes t_{(1)})$.

Definizione 1.4.9. Sia H una Hopf-algebra e sia R una $k-$algebra ed un $H-$comodulo. R è una $H-$*comodulo algebra* se le mappe M_R e u_R che definiscono la sua struttura come algebra sono morfismi di $H-$comoduli.

Abbiamo già visto che nel caso in cui H sia finitamente generata allora se R è un $H-$ modulo sinistro allora è anche un H^*-comodulo destro e viceversa e si può verificare facilmente che nel caso in cui R sia un'algebra se è dotata di una struttura di $H-$modulo algebra allora può essere dotata canonicamente di una struttura di H^*-comodulo algebra. Tale affermazione segue immediatamente da come abbiamo definito le mappe su H^* a partire da quelle di H le quali trasformano M_R e u_R da morfismi di $H-$moduli in morfismi di $H-$comoduli.

Capitolo 2

Teoria di Galois e struttura di Hopf-Galois

Scopo principale di questo capitolo sarà estendere tramite l'uso delle Hopf-algebre la teoria di Galois classica che si vede nei corsi unversitari dei primi anni ed introdurre i principali strumenti che verranno usati nel successivo capitolo per dimostrare alcuni teoremi che renderanno tali strutture interessanti e degne di studio.

2.1 Teoria di Galois classica

Partiamo da un breve ripasso della teoria di Galois, ci limiteremo al caso finito, quindi in tutta questa sezione e nelle successive L e k saranno due campi, in particolare L sarà un'estensione finita di k.

Definizione 2.1.1. Un elemento $a \in \bar{k}$ si dice *separabile* se il suo polinomio minimo ha tutte radici distinte (dove $\bar{k}$ è la chiusura algebrica di k).

Definizione 2.1.2. Un'estensione L/k algebrica si dice *separabile* se $\forall a \in L, a$ è separabile su k.

Definizione 2.1.3. Un'estensione L/k si dice *normale* se $\forall \varphi : L \to \bar{L}$ tali che $\varphi|_k = Id.$ si ha che $\varphi(L) = L$.

Definizione 2.1.4. Un'estensione L/k si dice di *Galois* se è normale e separabile.

Nel caso di estensioni di Galois si può parlare del gruppo di Galois dell'estensione denominato con $Gal(L/k)$ che sarà l'insieme degli endomorfismi da L in L che ristretti a k sono l'identità. Nel caso finito, che sarà l'unico che noi studieremo c'è una corrispondenza biunivoca tra i sottogruppi del gruppo di Galois e le

sottoestensioni, vedremo che in alcuni casi tale corrispondenza vale anche nel caso di estensioni di Hopf-Galois.

Nelle sezioni successive, data un'estensione di Galois L/k indicheremo con G il gruppo di Galois di tale estensione laddove ciò non sia fraintendibile.

2.2 Struttura di Hopf-Galois

Il nostro scopo è quello di definire una struttura su alcune estensioni finite anche non di Galois che ci permetta di descrivere tramite una Hopf-algebra i suoi endomorfismi, cioè sostanzialmente quello che nelle estensioni di Galois viene fatto dal gruppo di Galois. In particolare ci soffermeremo solo sulle estensioni separabili ed indicheremo con $End_k(L)$ gli endomorfismi di L come $k-$spazio vettoriale.

Per prima cosa notiamo che ovviamente se L/k è un'estensione di campi allora L è una $k-$algebra, inoltre se H è una Hopf-algebra e L è una $H-$modulo algebra sinistra possiamo dotare $L \otimes H$ di una struttura di $k-$algebra oltre che nella maniera canonica (il prodotto tensore di due algebre è un'algebra) anche attraverso un'altra definizione di prodotto, indicheremo tale algebra con $L\#H$ e definiremo la moltiplicazione come $(s\#x)(t\#y) = \sum_{(x)} sx_{(1)}(t)\#x_{(2)}y$ dove per non appesantire la notazione non sono state indicate le mappe di moltiplicazione su L e su H.

Definizione 2.2.1. Sia L/k un'estensione finita di campi ed H una $k-$Hopf-algebra. L si dice una *estensione* $H-$*Galois* o semplicemente $H-$*Galois* se L è una $H-$modulo algebra e il morfismo di moduli $j : L \otimes H \to End_k(L)$ definito come

$$j(l \otimes h)(t) = lh(t)$$

è in realtà un isomorfismo di algebre (dove $L \otimes H$ è dotato della struttura di algebra data da $\#$).

Esempio 2.2.2 (Estensioni di Galois classiche)**.** Vogliamo far vedere che, nel caso in cui l'estensione L/k sia di Galois, prendendo come Hopf-algebra kG otteniamo una estensione $kG-$Galois quindi in un certo senso stiamo davvero generalizzando la nozione classica. Sappiamo già che kG è una Hopf-algebra, dobbiamo quindi solo far vedere che il morfismo j della definizione è un'isomorfismo, avendo anche già visto che L è una kG-modulo algebra. L'iniettività di j è un semplice corollario del teorema di indipendenza dei caratteri di Artin. A questo punto concludiamo per motivi dimensionali. Infatti entrambe le nostre algebre sono $k-$spazi vettoriali della stessa dimensione quindi otteniamo immediatamente che il morfismo considerato essendo iniettivo deve anche essere suriettivo.

Una grossa differenza però tra le estensioni di Galois classiche e quelle Hopf-Galois è che non vale più l'unicità. Ovvero più Hopf-algebre possono dare origine

a strutture $H-$Galois diverse della stessa estensione L/k. Ciò vale anche nel caso di estensioni di Galois in cui cioè esiste anche una Hopf-algebra diversa da kG che rispetta la definizione nel caso in cui G sia non abeliano. Verranno fatti esempi di queste situazioni nel capitolo 4 dopo che si sarà studiato un modo per trovare le Hopf-algebre di Galois di una certa estensione.

Proposizione 2.2.3. *Se j è un isomorfismo allora il campo fisso $L^H = \{l \in L \mid h(l) = \epsilon(h)l \ \forall h \in H\} = k$.*

Dimostrazione. Per prima cosa notiamo che è evidente che $k \subseteq L^H$, sia infatti $x \in k$ allora $h(x) = xh(1) = x\epsilon(h)$ per definizione di $H-$modulo algebra.

Sia invece $l \in L^H$ mostriamo che l'elemento $l\#1$ commuta con tutti gli elementi di $L\#H$. Infatti sia $s\#h \in L\#H$ allora per definizione (ricordando che $\Delta(1) = 1 \otimes 1$ perchè H è una bialgebra)

$$\begin{aligned}(s\#h)(l\#1) &= \sum_{(h)} sh_{(1)}(l)\#h_{(2)} = \sum_{(h)} s\epsilon(h_{(1)})l\#h_{(2)} = \\ &= sl\sum_{(h)} \epsilon(h_{(1)})\#h_{(2)} = sl(\epsilon \otimes I)\Delta(h) = sl(1\#h) = \\ &= sl\#h = (l\#1)(s\#h)\end{aligned}$$

Dove nella prima riga abbiamo usato che $l \in L^H$ mentre nell'ultimo passaggio della seconda riga il secondo diagramma commutativo delle coalgebre.

Segue allora che $j(l\#1)$ commuta con tutti gli elementi di $End_k(L)$ dato che j è un isomorfismo, ma $j(l\#1)$ è la moltiplicazione per l quindi per commutare con tutti gli endomorfismi deve necessariamente essere $l \in k$. □

Chiaramente dato che abbiamo richiesto che l'estensione L/k sia finita allora anche l'H Hopf-algebra sarà finita ed abbiamo notato nel capitolo precedente che se L è una $H-$modulo algebra sinistra allora è anche una H^*-comodulo algebra destra e viceversa.

Diamo ora un'altra definizione che vedremo subito essere equivalente a quella data ma in cui invece di guardare l'azione di H su L guarderemo quella di H^*. Se L è una H^*-comodulo algebra destra sia $\alpha : L \to L \otimes H^*$ la mappa che definisce la struttura di comodulo.

Definizione 2.2.4. L è un H^*-oggetto di Galois se la mappa $\gamma : L \otimes L \to L \otimes H^*$ definita da:

$$\gamma(s \otimes t) = (s \otimes 1)\alpha(t)$$

è un isomorfismo.

Proposizione 2.2.5. *Sia H una Hopf-algebra e L/k un'estensione di campi finita, allora L è $H-$Galois se e solo se è un H^*-oggetto di Galois.*

Dimostrazione. Siano γ, α, j definiti come sopra. Abbiamo visto che se L è una $H-$modulo algebra allora è anche una H^*-comodulo algebra e viceversa dato che siamo nel caso finito dimensionale. Dobbiamo quindi dimostrare solo che se j è un isomorfismo allora lo è anche γ e viceversa. Per fare questo consideriamo il seguente diagramma:

$$\begin{array}{ccc} L \otimes H & \xrightarrow{\quad j \quad} & End_k(L) \\ \Big\downarrow \eta & & \Big\downarrow \beta \\ Hom_L(L \otimes H^*, L) & \xrightarrow{\gamma^*} & Hom_L(L \otimes L, L) \end{array}$$

dove $\eta(l \otimes h)(t \otimes f) = ltf(h)$ e $\beta(f)(l \otimes t) = lf(t)$ sono due isomorfismi, infatti gli spazi di arrivo e partenza hanno la stessa dimensione e l'iniettività è ovvia.

Definiamo inoltre $\gamma^*(f)(l \otimes t) = f(\gamma(l \otimes t))$ segue quindi che γ^* è un isomorfismo se e solo se lo è γ. Se dimostrassi quindi che il diagramma è commutativo avrei la tesi.

Sia quindi $l \otimes h \in L \otimes H$.

$$\beta \circ j(l \otimes h)(t \otimes u) = tj(l \otimes h)(u) = tlh(u)$$

$$\begin{aligned} \gamma^* \circ \eta(l \otimes h)(t \otimes u) &= \eta(l \otimes h)(\gamma(t \otimes u)) = \eta(l \otimes h)((t \otimes 1)\alpha(u)) = \\ &= \eta(l \otimes h)((t \otimes 1)(\sum_{(u)} u_{(0)} \otimes u_{(1)})) = \eta(l \otimes h)(\sum_{(u)} tu_{(0)} \otimes u_{(1)}) = \\ &= lt \sum_{(u)} u_{(0)}u_{(1)}(h) = lth(u) \end{aligned}$$

Dove l'ultima uguaglianza deriva da come definiamo la mappa α a partire dalla struttura di $H-$modulo.

□

2.3 Estensione del campo degli scalari

Sia L un'estensione $H-$Galois di k e sia E un'altra estensione finita di k. Un fatto noto e che si verifica facilmente è che $E \otimes L$ ha una naturale struttura di spazio vettoriale su E dove la moltiplicazione per un elemento di E è data semplicemente moltiplicando le prime componenti per tale elemento; è quindi una $E-$algebra dato che possiamo anche definire una moltiplicazione componente per componente.

Proposizione 2.3.1. *Nelle ipotesi precedenti $E \otimes L$ è un'estensione $E \otimes H$-Galois di E.*

Dimostrazione. Per prima cosa, affinchè la tesi abbia senso dobbiamo notare che $E \otimes H$ è una Hopf-algebra. Ma questa è una semplice verifica che deriva dal fatto che essendo E un'estensione finita di k è in particolare un modulo piatto, quindi tensorizzando si conservano tutte le successioni esatta, ma allora anche i diagrammi commutativi che mi definivano la struttura di Hopf-algebra.

Anche il fatto che $E \otimes L$ sia una $E \otimes H-$modulo algebra deriva immediatamente dalla piattezza di E.

L'unica verifica non ovvia è che $J : (E \otimes_k L) \otimes_E (E \otimes_k H) \to End_E(E \otimes_k L)$ sia un isomorfismo sapendo che $j : L \otimes_k H \to End_k(L)$ lo è. Usando le proprietà del prodotto tensore otteniamo però che:

$$(E \otimes_k L) \otimes_E (E \otimes_k H) = (L \otimes_k E) \otimes_E (E \otimes_k H) = L \otimes_k (E \otimes_E E) \otimes_k H = \\ = L \otimes_k E \otimes_k H = L \otimes_k H \otimes_k E$$

che per piattezza è isomorfo a $End_k(L) \otimes_k E$. Ma quest'ultimo è isomorfo a $End_E(E \otimes_k L)$, infatti quest'ultimo isomorfismo vale in generale per moduli proiettivi quindi nel nostro caso in cui abbiamo spazi vettoriali, quindi moduli liberi è ovvio, si vede poi che l'isomorfismo conserva il prodotto quindi passa alle algebre. □

Questa proposizione risulterà molto importante nei capitoli successivi nei quali infatti estenderemo il campo degli scalari per ottenere dei campi nei quali è più facile vedere come sono fatte le Hopf-algebre di Galois e, anche usando la teoria di Morita di cui parleremo nella sezione successiva, riusciremo a tornare indietro e a individuare le varie forme che può avere la Hopf-algebra di Galois di partenza.

2.4 Teoria di Morita e discesa di Galois

Sia L un'estensione di Galois finita di k, abbiamo già detto che L è una $k-$algebra. Se inoltre A è un altro $k-$spazio vettoriale allora $L \otimes A$ è a sua volta un $L-$spazio vettoriale e similmente nel caso in cui A sia una $k-$algebra o $k-$Hopf-algebra. Dati inoltre A e B $k-$spazi vettoriali, se abbiamo un morfismo di $k-$spazi vettoriali f tra di loro riusciamo ad ottenere un morfismo di $L-$spazi vettoriali dopo aver esteso il campo degli scalari con L operando solo sulla seconda componente. Chiameremo tale morfismo $L \otimes f$ dove $(L \otimes f)(l \otimes a) = l \otimes f(a)$.

La teoria della discesa studia il problema inverso, ovvero, dato un $L-$spazio vettoriale A si chiede quando esso sia della forma $L \otimes_k A_0$ dove A_0 è un $k-$spazio vettoriale oppure, quando dato un morfismo di $L-$moduli $f : L \otimes_k A_0 \to L \otimes_k B_0$, esso è della forma $L \otimes f_0$ per un qualche morfismo di $k-$moduli $f_0 : A_0 \to B_0$.

La teoria di Morita dà una risposta parziale a questo interrogativo.

Teorema 2.4.1. *([4, teorema 3.54]) Sia A una $R-$algebra e $B = End_k(A)$ esiste allora un'equivalenza di categorie tra la categoria degli $R-$moduli sinistri e la categoria dei $B-$moduli sinistri dove l'equivalenza è data dal funtore $A \otimes_R *$ in un verso e dal funtore $Hom_E(A, E) \otimes_B *$ nell'altro.*

Usando il teorema otteniamo che un $L-$spazio vettoriale M è della forma $L \otimes M_0$ per un certo $k-$spazio vettoriale M_0 se e solo se riusciamo ad estendere l'azione di L su M ad un'azione di $End_k(L)$.

Ci chiediamo ora, nel caso specifico che ci interessa, ovvero di una estensione di Galois, cosa succede. Abbiamo visto che $End_k(L)$ è isomorfo a $L \otimes kG \cong LG$, quindi un $End_k(L)-$modulo sinistro è semplicemente un $L-$modulo sinistro dotato di un'azione di G compatibile. In questo caso riusciamo allora a scriverci espressamente come è fatto M_0, ciò vale in generale per estensioni Hopf-Galois.

Lemma 2.4.2. *Sia L/k un'estensione $H-$Galois e sia $E = End_k(L)$. Ogni $E-$modulo M è isomorfo a $L \otimes M^H$ (dove M^H è un $k-$modulo) tramite la mappa $f(l \otimes m) = lm$.*

Dimostrazione. Per il teorema precedente c'è un'equivalenza tra i $k-$moduli e gli $E-$moduli e sappiamo le mappe che danno l'equivalenza. Sia quindi M un $E-$modulo, segue che $M \cong L \otimes_k Hom_E(L, E) \otimes_E M$.

Notiamo però ora che $Hom_E(L, E) \otimes_E M \cong Hom_E(L, M)$. Questo isomorfismo è ovvio nel caso in cui $L \cong E^n$ ovvero se è un $E-$modulo libero ma allora vale anche per addendi diretti di moduli liberi quindi in particolare per moduli proiettivi. Ma L è appunto un $E-$modulo proiettivo essendo $E \cong L^{n^2}$ dove n è la dimensione di L come $k-$spazio vettoriale.

Usando ora il fatto che l'estensione è $H-$Galois otteniamo che $Hom_E(L, M) \cong Hom_{L\#H}(L, M)$. Resta quindi solo da dimostrare che $Hom_{L\#H}(L, M) \cong M^H$ tramite l'isomorfismo che manda ϕ in $\phi(1)$. Infatti ϕ è univocamente determinata dalla sua immagine dato che $\phi(s) = \phi((s\#1)1) = (s\#1)\phi(1)$. Inoltre l'immagine è proprio in M^H: dato $h \in H$

$$h\phi(1) = (1\#h)\phi(1) = \phi((h\#1)1) = \phi(\epsilon(h)1) = \epsilon(h)\phi(1)$$

dove $(h\#1)1 = \epsilon(h)$ è una delle due proprietà delle modulo algebre.

Abbiamo quindi detto che la mappa è ben definita, inoltre per come l'abbiamo costruita è anche necessariamente iniettiva, l'unica cosa che dobbiamo ancora dire è la surgettività, ma dato $m \in M^H$ se definiamo $\phi \in Hom_{S\#H}(L, M)$ come $\phi(s) = sm$ abbiamo chiaramente che $\phi(1) = m$ ed essa è ben definita.

□

Ritorniamo ora di nuovo al caso di estensioni di Galois classiche. Abbiamo sostanzialmente studiato la discesa nel caso dei moduli, vogliamo quindi adesso vedere cosa succede ai morfismi. Supponiamo che A e B siano due $LG-$moduli e sia inoltre $f : A \to B$ un morfismo di $L-$moduli che sia $G-$equivariante, ovvero tale che $f(\sigma(a)) = \sigma(f(a))$ per ogni $\sigma \in G$ e $a \in A$. Segue immediatamente che f è un morfismo di $LG-$moduli e quindi è della forma $L \otimes f_0$. Infatti è sufficiente definire f_0 come $f|_{A^G}$ e $f(l \otimes m) = l \otimes f(m) = l \otimes f_0(m)$.

Vorremmo adesso far vedere che se A ha delle strutture aggiuntive esse vengono preservate in A^G. In particolare il caso che ci interessa è quello in cui A è una $L-$Hopf-algebra e supponiamo che G agisca su A come morfismo di Hopf-algebre. In questo caso otteniamo che A^G è una $k-$Hopf-algebra infatti il funtore $(*)^G$ manda i diagrammi commutativi in diagrammi commutativi quindi tutto viene preservato.

Allo stesso modo se H è una $L-$Hopf-algebra e A una $H-$modulo algebra, ed abbiamo inoltre un gruppo G che agisce su H e A rispettandone le strutture e la funzione che definisce il modulo è $G-$equivariante segue allora che A^G è una H^G-modulo algebra.

Capitolo 3

Teorema di Greither

In questo capitolo arriveremo a dimostrare, nell'ultima sezione, un teorema dovuto a Greither e Pareigis che permette di calcolare esplicitamente tutte le diverse strutture Hopf-Galois di una certa estensione separabile a patto di conoscerne il gruppo di Galois della chiusura normale e poco altro. I riferimenti principali saranno l'articolo originale di Greither e Pareigis [3] e il testo di Childs [2].

3.1 Hopf-Galois strutture su XE

In tutta questa sezione X sarà un'insieme ed indicheremo con XL le mappe da X a L dove L è un campo. Sarà inoltre $Perm(X)$ il gruppo delle permutazioni di X.

Definizione 3.1.1. Un sottogruppo N di $Perm(X)$ è detto regolare se soddisfa due delle seguenti tre condizioni:

- N e X hanno la stessa cardinalità;
- N agisce in maniera transitiva su X (cioè per ogni coppia di elementi $x, y \in X$ esiste un elemento η di N tale che $\eta(x) = y$);
- $Stab_N(x) = \{\eta \in N | \eta(x) = x\} = \{Id.\}$ per ogni elemento $x \in X$.

Risulta chiaro che se un sottogruppo soddisfa due delle tre condizioni precedenti allora soddisfa anche la terza. In particolare stiamo dicendo che un sottogruppo N è regolare se fissando un qualunque elemento di X e guardando l'azione di N su tale elemento otteniamo una bigezione tra N e X stesso.

Guardiamo ora XL come $L-$algebra dove la moltiplicazione è data dal prodotto delle immagini. Definiamo $u_x : X \to L$ come $u_x(y) = \delta_x^y$ per ogni $y \in X$. Notiamo che l'insieme $\{u_x | x \in X\}$ è una $L-$base di XL composta da elementi

idempotenti e tali che $u_x u_y = 0$ se $x \neq y$. Siamo ora in grado di enunciare il teorema che caratterizza le Hopf-strutture sull'estensione XL/L e che successivamente ci permetterà di classificare le Hopf-algebre su estensioni separabili qualsiasi.

Teorema 3.1.2. *Sia X un insieme finito e L un campo. Se H è una Hopf-algebra tale che XL è un'estensione $H-$Galois di L, allora H è l'algebra di gruppo LN per un qualche N della stessa cardinalità di X. N può essere identificato con un sotogruppo di $Perm(X)$ dove l'azione di N su X è definita da $u_{\eta(x)} = \eta(u_x)$ per ogni $x \in X$ e $\eta \in N$. N è allora un sottogruppo regolare di $Perm(X)$. Viceversa se N è un sottogruppo regolare di $Perm(X)$, allora XL è $LN-$Galois.*

Dimostrazione. Supponiamo che XL sia $H-$Galois e X sia un insieme di n elementi. Vale allora la seguente catena di isomorfismi come $L-$algebre:

$$\begin{aligned} L \times \cdots \times L \ (n^2 \ volte) \cong Map(X \times X, L) &\cong XL \otimes_L XL \\ &\cong XL \otimes_L H^* \cong H^* \times \cdots \times H^* \ (n \ volte) \end{aligned}$$

dove il passaggio dalla prima alla seconda riga è dato dallo proposizione 2.2.5 e gli altri isomorfismi sono ovvi. Ma da questo segue immediatamente che come $L-$algebra $H^* \cong L \times \cdots \times L$ (n *volte*). Sia quindi $\eta_i : H^* \to L$ la proiezione sulla $i-$esima coordinata. Vale allora che $N = \{\eta_i\}$ è una base di $H^{**} \cong H$.

Segue da come abbiamo definito nel primo capitolo la coalgebra duale che $\Delta(\eta_i) = \eta_i \otimes_L \eta_i$. Notiamo inoltre che N è un gruppo infatti gli elementi di N sono gli unici elementi grouplike di H dato che gli altri sono combinazioni lineari di questi e si vede che non possono esserlo. Ma l'insieme degli elementi grouplike di una Hopf-algebra è un gruppo; dati infatti h, j grouplike $\Delta(hj) = \Delta(h)\Delta(j) = (h \otimes h)(j \otimes j) = hj \otimes hj$ e similmente si verifica che c'è l'inverso usando la mappa antipodale.

Dalle due osservazioni precedenti segue quindi che H è l'algebra di gruppo LN. Vogliamo ora dimostrare che N agisce come un gruppo di permutazioni di X.

Sia $\{u_x\}$ la base di idempotenti di XL definita sopra. Dato che XL è una $LN-$modulo algebra essendo un'estensione Hopf-Galois vale che

$\eta_i(u_x) = \eta_i(M(u_x \otimes u_x)) = \Delta(\eta_i(u_x) \otimes \eta_i(u_x)) = \eta_i(u_x)^2$ inoltre $0 = \eta_i(u_x u_y) = \eta_i(u_x)\eta_i(u_y)$. Quindi ciascun elemento di N manda una base di idempotenti ortogonali di XL in una base di idempotenti ortogonali di XL. Si vede immediatamente però che gli unici elementi idempotenti di XL sono somme finite di alcuni u_x con coefficienti 1. Ma infine vale anche che:

$$1 = \eta_i(1) = \eta_i(\sum_{x \in X} u_x) = \sum_{x \in X} \eta_i(u_x)$$

da cui segue che η_i permuta gli elementi della forma u_x dato che nessuno può comparire più di una volta ma allora η_i posso anche vederlo come elemento di $Perm(X)$ (dove $\eta_i(x) = y$ se $\eta_i(u_x) = u_y$).

Dobbiamo ora mostrare che N è un sottogruppo regolare ma questo è facile infatti sicuramente N e X hanno la stessa cardinalità. Inoltre dal fatto che XL è $LN-$Galois segue immediatamente che l'azione di N su X è transitiva.

Per quanto riguarda il viceversa si tratta di fare delle semplici verifiche utilizzando le stesse notazione date nella dimostrazione.

Infatti chiamiamo per prima cosa con l_{xz} l'elemento di $End_L(XL)$ tale che $l_{xz}(u_x) = u_z$ mentre $l_{xz}(u_y) = 0$ per ogni $y \neq x$. Questi elementi formano chiaramente una base. Utilizzando ora il fatto che N è regolare, dato $z, x \in X$ esisterà $\eta \in N$ tale che $\eta(x) = y$. Definiamo allora una mappa j tale che $j(u_z \otimes \eta) = l_{xz}$. Per linearità riusciamo ad estendere la mappa j ad un morfismo $\bar{\jmath}$: $XL \otimes LN \to End_L(XL)$. Per quanto abbiamo già detto tale mappa è suriettiva inoltre dato che X e N hanno la stessa cardinalità anche i due spazi vettoriali hanno la stessa dimensione quindi tale mappa è una biezione. □

Forti di questo teorema nella prossima sezione cercheremo di estendere il nostro campo in modo da ottenerne uno della forma XL per un qualche insieme finito X per poter studiare lì le sue strutture di Hopf-Galois.

3.2 Alcuni lemmi preparatori

Sia L un'estensione finita e separabile di k dove k è un campo. Il nostro obiettivo sarà quello di cercare di collegarci al teorema dimostrato nella sezione precedente. Chiameremo E la chiusura normale di L/k, $G = Gal(E/k)$ e $G' = Gal(E/L)$; chiameremo infine $X = G/G'$ l'insieme delle classi laterali sinistre. Notiamo che XE può essere dotato di una struttura di $G-$modulo tramite l'azione $\tau(f)([\sigma]) = \tau(f([\tau^{-1}\sigma]))$ dove $\tau \in G$, $[\sigma] \in X$ e $f \in XE$. Inoltre chiaramente anche $E \otimes L$ è un $G-$modulo dove $\tau(e \otimes l) = \tau(e) \otimes l$, vale quindi la seguente proposizione:

Proposizione 3.2.1. *La mappa $\gamma : E \otimes L \to XE$ definita da $\gamma(e \otimes l)([\sigma]) = e\sigma(l)$ dove σ è un qualunque rappresentante della classe $[\sigma]$ è un isomorfismo di E-algebre e G-moduli.*

Dimostrazione. Intanto la buona definizione della mappa γ ed il fatto che essa sia un morfismo di $E-$algebre e di $G-$moduli sono semplici verifiche. Notiamo inoltre che sia il dominio che il codominio hanno la stessa dimensione visti come $k-$spazi vettoriali, quindi per dimostrare che γ è veramente un isomorfismo basta ad esempio dimostrarne l'iniettività.

Siano $\{e_1, \dots, e_n\}$ una $k-$base di E, ovviamente qualunque elemento di $E \otimes L$ possiamo scriverlo come $e_1 \otimes l_1 + \cdots + e_n \otimes l_n$ dove $l_1, \dots, l_n \in L$. Supponiamo per assurdo che un elemento di tale forma appartenga al Ker, allora per come abbiamo definito γ vale che $\forall \sigma \in G : e_1\sigma(l_1) + \cdots + e_n\sigma(l_n) = 0$. Chiamando

$k_i = Tr(l_i)$ dove con tale notazione intendiamo la traccia di E/k e sommando tutte le equazioni otteniamo $k_1e_1 + \cdots + k_ne_n = 0$ che è assurdo avendo supposto gli e_i una base di E. □

Quindi in un certo senso ci siamo ricondotti al teorema precedente.

Notiamo ora che esiste una ovvia immersione di G dentro $Perm(X)$ data da λ dove dati $\tau \in G$ e $[\sigma] \in X$ vale $\lambda(\tau)([\sigma]) = [\tau\sigma]$. Abbiamo detto che tale mappa è un'immersione, che sia infatti un omomorfismo di gruppi è una facile verifica, inoltre supponiamo per assurdo che abbia Ker non banale, sia quindi $Ker\lambda = M$. Sicuramente, dato che gli elementi di M fissano tutte le classi laterali fisseranno anche la classe $[e]$ dove e è l'identità del gruppo, ma questo implica immediatamente che $M \subseteq G'$. Inoltre essendo M un Ker è sicuramente normale, segue quindi che E^M è un sottocampo normale di E che contiene L ma allora E non era la chiusura normale.

Siamo ora pronti a dimostrare un lemma che ci porterà molto vicini all'enunciato finale del teorema.

Lemma 3.2.2. *Sia L/k un'estensione $H-$Hopf-Galois, utilizzando le notazioni precedenti abbiamo che $E\otimes H \cong EN$ dove N è un sottogruppo regolare di $Perm(X)$ normalizzato da $\lambda(G)$.*

Dimostrazione. Abbiamo già visto che se L è un'estensione $H-$Galois di k allora $E \otimes_k L$ è un'estensione $E \otimes_k H-$Galois di E. Inoltre per la proposizione 3.2.1 $E \otimes_k L \cong XE$ quindi per il teorema 3.1.2 $E \otimes_k L \cong EN$ dove N è un sottogruppo regolare di $Perm(X)$. L'unica cosa che resta da dimostrare è che in questo caso N è normalizzato da $\lambda(G)$.

Ricordando la dimostrazione del teorema 3.1.2 e ricordandoci che siamo nel caso particolare in cui $X = G/G'$ possiamo prendere come base di XE come $E-$spazio vettoriale gli elementi $\{u_{\bar\sigma} \mid \bar\sigma \in X\}$ dove ricordiamo che dati $\bar\sigma, \bar\tau \in X$ vale $u_{\bar\sigma}(\bar\tau) = \delta_{\bar\sigma,\bar\tau}$, dove la δ è la delta di Kronecker. Abbiamo inoltre definito un'azione di G su XE; restringendo tale azione agli elementi della base scelta otteniamo che, dati $\tau \in G$, $[\sigma], [\rho] \in X$:

$$\tau(u_{[\sigma]}([\rho]) = \tau(u_{[\sigma]}([\tau^{-1}\rho])) = u_{[\sigma]}([\tau^{-1}\rho]) = u_{[\tau\sigma]}([\rho]) = u_{\lambda(\tau)[\sigma]}([\rho])$$

Quindi l'azione di G sulla base scelta corrisponde ad una traslazione sinistra delle classi laterali. Inoltre, sempre ricordando il teorema precedente avevamo che $\eta \in N$ agisce sugli elementi della base tramite $\eta(u_{[\sigma]}) = u_{\eta([\sigma])}$, dove stiamo in questo momento vedendo N come immerso in $Perm(X)$.

Notiamo ora che l'azione che definisce la struttura di modulo algebra:

$(E \otimes_k H) \otimes_E (E \otimes_k L) \to E \otimes_k L$ è ovviamente $G-$equivariante, dove G agisce su E, lasciando invariata la seconda componente di tutti i prodotti tensori.

Inoltre abbiamo anche già osservato che l'isomorfismo $E \otimes_k L \cong XE$ è anche un isomorfismo di $G-$moduli, segue allora che l'azione $EN \otimes_E XE \to XE$ è anch'essa $G-$equivariante. Usando questo fatto siamo pronti a definire qual è l'azione di G sugli elementi di EN, in particolare ci limitiamo agli elementi di N che sono quelli che ci interessano.

Il nostro obiettivo sarà far vedere che G agisce su N tramite coniugio visti come elementi di $\lambda(G)$, a quel punto avremo la tesi.

Sia quindi $\tau \in G$, $\eta \in N$, $[\sigma] \in X$. Il fatto che la mappa scritta sopra sia $G-$equivariante equivale a dire che:

$$\tau(\eta)\tau(u_{[\sigma]}) = \tau(\eta(u_{[\sigma]})) = \tau(u_{\eta([\sigma])})$$

Valgono tuttavia le seguenti facili uguaglianze:

$$\tau(\eta)\tau(u_{[\sigma]}) = u_{\tau(\eta)(\lambda(\tau)([\sigma]))}$$
$$\tau(u_{\eta([\sigma])}) = u_{\lambda(\tau)\eta([\sigma])}$$

Quindi: $\tau(\eta)(\lambda(\tau)([\sigma])) = \lambda(\tau)\eta([\sigma])$ da cui segue che:

$$\tau(\eta)([\sigma]) = \lambda(\tau)\eta\lambda(\tau^{-1})([\sigma])$$

□

3.3 Teorema principale e sua dimostrazione

Usando quanto detto nelle due sezioni precedenti, ed in particolare utilizzando le stesse notazioni, siamo ora pronti ad enunciare e dimostrare il teorema di Greither e Pareigis.

Teorema 3.3.1. *Sia L/k un'estensione finita e separabile di campi con chiusura normale E e sia $G = Gal(E/k)$, $G' = Gal(E/L)$, $X = G/G'$. Esiste allora una bigezione tra i sottogruppi regolari N di $Perm(X)$ normalizzati da $\lambda(G)$ e le Hopf-Galois strutture su L/k.*

Dimostrazione. Abbiamo già visto nel teorema precedente che se N è un sottogruppo regolare di $Perm(X)$ allora XE è un'estensione $EN-$Galois di E. Dove quindi per la definizione di estensione Hopf-Galois sia EN che XE sono $E-$moduli e inoltre XE è una $EN-$modulo algebra, cioè l'azione $\phi : EN \otimes_E XE \to XE$ è un morfismo di $E-$moduli. Quello che noi vorremmo fare ora è, ricordandoci che $XE \cong E \otimes_k L$, usare la teoria di Morita esposta nella sezione 2.4 per ottenere una struttura Hopf-Galois di L. In particolare per far vedere che ϕ è il sollevamento di un morfismo di $k-$moduli per quanto già visto è sufficiente far vedere che ϕ è un morfsmo di $End_k(E)-$moduli.

Poichè E/k è un'estensione di Galois con gruppo di Galois G vale che $End_k(E) = EG$ come abbiamo già notato, dobbiamo quindi verificare che l'azione di EG su EN e XE rende ϕ un morfismo di $EG-$moduli.

Per prima cosa vediamo quali sono le azioni di EG su EN e su XE. Dato $g \in G$, l'azione di tale elemento su XE l'abbiamo già vista ed è $g(f)([\tau]) = g(f(\lambda(g^{-1})([\tau])))$ mentre $e \in E$ agisce come $e(f)([\tau]) = e(f([\tau]))$ dove $f \in XE$ mentre $[\tau] \in X$. Allora un elemento di EG della forma eg agisce su XE tramite:

$$eg(f)([\tau]) = e(g(f(\lambda(g^{-1})([\tau])))) = e(g(f)([\tau]))$$

e rende XE un $EG-$modulo.

Inoltre abbiamo anche già visto come agisce G su EN ovvero dati $a \in E$ e $\eta \in N$ abbiamo che $g(a\eta) = g(a)g(\eta) = g(a)\lambda(g)\eta\lambda(g^{-1})$ ma allora un elemento $eg \in EG$ agisce su EN rendendolo un $EG-$modulo tramite:

$$eg(a\eta) = eg(a)\lambda(g)\eta\lambda(g^{-1})$$

Possiamo quindi finalmente passare a dimostrare che ϕ è un morfismo di $EG-$moduli. Dato che sappiamo già che è un morfismo di $E-$moduli ed utilizzando la linearità è sufficiente dimostrare che dato $g \in G$, $a\eta \in EN$ e $f \in XE$ vale:

$$\phi(g(a\eta \otimes f))([\tau]) = g(\phi(a\eta \otimes f))([\tau])$$

Si tratta di una semplice verifica in cui utilizziamo le formule scritte precedentemente per ricavare le due seguenti catene di uguaglianze, dove stiamo ovviamente supponendo che G agisca su $EN \otimes XE$ agendo su entrambe le componenti.

$$\begin{aligned}\phi(g(a\eta \otimes f))([\tau]) &= \phi(g(a\eta) \otimes g(f))([\tau]) = g(a)g(\eta)g(f)([\tau]) = \\ &= g(a)g(f)(g(\eta)^{-1}[\tau]) = g(a)g(f(\lambda(g^{-1})(g(\eta)^{-1}[\tau]))) = \\ &= g(a)g(f(\lambda(g^{-1})(\lambda(g)\eta^{-1}\lambda(g^{-}1)[\tau])))\end{aligned}$$

$$\begin{aligned}g(\phi(a\eta \otimes f))([\tau]) &= g(a\eta f([\tau]) = g(a)g(\eta f)(\lambda(g^{-1})[\tau]) = \\ &= g(a)g(f(\eta^{-1}(\lambda(g^{-1})[\tau])))\end{aligned}$$

Quindi le due scritture coincidono e ϕ è un morfismo di $EG-$moduli.

Ora, ricordandoci la teoria di Morita ed il fatto che siamo nel caso particolare studiato nella sezione 2.4 in cui E/k è un'estensione di Galois con gruppo di Galois G, abbiamo che esiste una corrispondenza biunivoca tra la categoria dei $k-$moduli e la categoria degli $EG-$moduli dove i due funtori che ci danno la corrispondenza sono rispettivamente il funtore di cambio di base: $M \to E \otimes_k M$ e il funtore di $G-$invarianza, ovvero:

$$N \to N^G = \{n \in N \mid g(n) = n \ \forall \ g \in G\}$$

Allora il morfismo ϕ di $EG-$moduli dà origine ad un unico morfismo φ di $E^G = k-$moduli dato dal funtore di $G-$invarianza, cioè:

$$\varphi : (EN)^G \otimes_k (XE)^G \to (XE)^G$$

Poichè l'azione di G su EN rispetta la struttura di Hopf-algebra di EN (cioè si verifica facilmente che tutte le mappe che definiscono la struttura di Hopf algebra Δ,ϵ,M,u,S sono anche morfismi di $EG-$moduli), segue che $(EN)^G$ è una $k-$Hopf-algebra.

Per lo stesso motivo, guardando l'azione di G su XE si vede che $(XE)^G$ è una $k-$algebra. Allo stesso modo dato che l'azione data da ϕ dava una struttura di $EN-$modulo algebra allora l'azione di φ darà origine ad una struttura di $(EN)^G-$modulo algebra.

Infine utilizzando l'altra freccia della corrispondenza data dalla teoria di Morita sappiamo che $E \otimes_k (EN)^G \cong EN$ e $E \otimes_k (XE)^G \cong XE$. Inoltre per ipotesi $j : XE \otimes_E EN \to End_E(XE)$ è un isomorfismo, ma allora scrivendolo come $j : (E \otimes_k (XE)^G) \otimes_E (E \otimes_k (EN)^G) \to End_E(XE)$ otteniamo che anche:

$$j_G : (XE)^G \otimes_k (EN)^G \to End_k((XE)^G)$$

è un isomorfismo. Cioè $(XE)^G$ è un'estensione $H-$Hopf-Galois di k, dove $H = (EN)^G$.

L'ultima cosa che ci resta da dimostrare è che $L \cong (XE)^G$ dove l'isomorfismo è dato dalla mappa f tale che, dato $l \in L$:

$$f(l) = \sum_{[\tau]\in X} \tau(l) u_{[\tau]}$$

Dove la buona definizione segue dal fatto che $\tau(l)$ non dipende dal rappresentante scelto e i $u_{[\tau]}$ sono i soliti elementi della base già incontrati, inoltre l'immagine che a priori è in XE si vede subito essere in realtà in $(XE)^G$, basta ricordarsi come agisce G su XE.

Inoltre f è ovviamente iniettiva dato che i $\{u_{[\tau]}\}$ sono una base di XE, l'unica cosa non ovvia da dimostrare è perciò la suriettività.

Sia quindi $\sum_{[\tau]\in X} e_{[\tau]} u_{[\tau]}$ un elemento qualsiasi di EN dove gli elementi $e_{[\tau]}$ sono elementi di E. Applicando $g \in G$ a tale elemento otteniamo che:

$$g(\sum_{[\tau]\in X} e_{[\tau]} u_{[\tau]}) = \sum_{[\tau]\in X} g(e_{[\tau]}) u_{[g\tau]}$$

Gli elementi di $(XE)^G$ sono quindi quelli tali che per ogni $g \in G$ e $[\tau] \in G/G'$ vale che: $g(e_{[\tau]}) = e_{[g\tau]}$. In particolare considerando la classe [1] otteniamo che

$e_{[1]} = g(e_{[1]}$ per ogni $g \in G'$ cioè $e_{[1]} \in E^{G'} = L$ ed inoltre che $e_{[g]} = g(e_{[1]}$ da cui la suriettività della mappa scritta.

Ricapitolando, abbiamo dimostrato che una struttura Hopf-Galois di XE/E data da una Hopf-algebra della forma EN dove N è un sottogruppo regolare di $Perm(X)$ normalizzato da $\lambda(G)$ corrisponde ad un'unica struttura Hopf-Galois di L/k. Tuttavia per il lemma 3.2.2 abbiamo che vale anche l'inverso cioè se L/k è un'estensione $H-$Hopf-Galois allora siamo in grado di associare a H un sottogruppo regolare e normalizzato da $\lambda(G)$ di $Perm(X)$.

Siamo quindi riusciti a dimostrare la corrispondenza biunivoca del teorema.

□

Notiamo che la dimostrazione ci permette di calcolare espressamente le Hopf-algebre che ci danno le varie strutture Hopf-Galois. Infatti, usando le stesse notazioni del teorema abbiamo che al sottogruppo regolare N corrisponde la Hopf-algebra $H = (EN)^G$ dove G agisce su N per coniugio visto come sottogruppo di $Perm(X)$.

Capitolo 4

Conseguenze del teorema ed esempi

In questo capitolo verranno presentati svariati esempi di utilizzo del teorema 3.3.1. Nella prima sezione verranno analizzate le estensioni di Galois classiche e si vedrà cosa si può dire in questo caso particolare. Nella seconda sezione invece vedremo come il teorema si comporti particolarmente bene per studiare le estensioni di piccolo grado, passando infine, nell'ultima sezione, a dare un esempio esplicito di suo utilizzo nel caso di un'estensione che ammette più di una struttura Hopf-Galois.

4.1 Caso estensioni di Galois classiche

Consideriamo il caso delle estensioni di Galois classiche. Utilizzando le notazioni del capitolo precedente otteniamo che in questo caso X sarà tutto G, cerchiamo quindi sottogruppi regolari di $Perm(G)$ normalizzati da $\lambda(G)$. Da cui otteniamo immediatamente che $\lambda(G)$ è un sottogruppo regolare che rispetta la tesi.

Tuttavia possiamo immergere G in $Perm(G)$ anche in un altro modo e continuare ad ottenere un sottogruppo regolare e precisamente tramite ρ tale che, dati $\tau, \sigma \in G$:

$$\rho(\sigma)(\tau) = \tau\sigma^{-1}$$

Si vede inoltre immediatamente che gli elementi di tale gruppo rimangono fissi sotto l'azione di $\lambda(G)$ quindi $\rho(G)$ è normalizzato anch'esso da $\lambda(G)$.

Vogliamo far vedere ora che nel caso in cui il gruppo di Galois sia non abeliano allora $\lambda(G) \neq \rho(G)$ quindi come già anticipato abbiamo almeno due strutture Hopf-Galois distinte. Intanto è facile vedere che se il gruppo è abeliano allora le due immersioni coincidono infatti abbiamo che $\lambda(\sigma) = \rho(\sigma^{-1})$. Leggermente più complicato è invece far vedere l'altra implicazione.

Supponiamo quindi che $\lambda(G) = \rho(G)$, allora dato $\sigma \in G$ deve esistere $\pi \in G$ tale che $\rho(\sigma) = \lambda(\pi)$. Ma se li valutiamo in $e \in G$ otteniamo che $\rho(\sigma)(e) = \sigma^{-1} = \pi = \lambda(\pi)(e)$ cioè deve necessariamente essere $\pi = \sigma^{-1}$. Se ora supponiamo che il gruppo G sia non abeliano esistono $\sigma, \tau \in G$ tali che $\sigma\tau \neq \tau\sigma$ da cui:

$$\lambda(\sigma^{-1})(\tau) = \sigma^{-1}\tau \neq \tau\sigma^{-1} = \rho(\sigma)(\tau)$$

da cui abbiamo la tesi.

Quando abbiamo introdotto le strutture Hopf-Galois avevamo immediatamente notato che su estensioni di Galois classiche si trova immediatamente che l'Hopf-algebra kG ci dà una struttura Hopf-Galois, viene quindi spontaneo chiedersi se tale struttura venga messa in relazione dal teorema con uno dei due sottogruppi appena trovati. La risposta è affermativa.

Proposizione 4.1.1. *$\rho(G) \in Perm(G)$ corrisponde all'azione classica di G su L.*

Dimostrazione. La dimostrazione di questo fatto si basa sulla dimostrazione del teorema 3.3.1 nella quale viene data esplicitamente l'azione di un gruppo regolare N di $Perm(X)$ su L. Nel nostro caso $N = \rho(G)$ e dato che abbiamo fatto notare che $\lambda(G)$ commuta con $\rho(G)$ otteniamo che $H = (LN)^{\lambda(G)} = L^G N = kN$. Sempre guardando la dimostrazione vediamo che l'azione di kN su L è indotta da quella di kN su $(GL)^{\lambda(G)} = \{\sum_\tau \tau(s)u_\tau \mid s \in L\}$.

Ma se $l \in L$ corrisponde a $\sum \tau(s)u_\tau \in GL$, allora per $\sigma \in G$ vale che: $\rho(\sigma)(\sum \tau(s)u_\tau) = \sum \tau(s)u_{\tau\sigma^{-1}} = \sum \tau\sigma(s)u_\tau$. Ma quest'ultimo corrisponde a $\sigma(l)$ in L, abbiamo quindi ottenuto come volevasi dimostrare che l'azione indotta da $\rho(G)$ è proprio quella classica. □

Vogliamo ora trovare in un esempio a quale struttura Hopf-Galois corrisponde invece il sottogruppo $\lambda(G)$.

Esempio 4.1.2. Sia $G = S_3$ generato da due elementi σ e τ rispettivamente un 3-ciclo ed una trasposizione. Supponiamo quindi di avere un'estensione di Galois classica L/k che abbia G come gruppo di Galois. Chiameremo $N = \lambda(G)$ e usando il teorema 3.3.1 vogliamo trovare l'Hopf-algebra H corrispondente.

Sappiamo che $H = (LN)^{\lambda(G)}$ cioè, identificando $\lambda(G)$ con G, $H = \{\epsilon \in LN \mid \epsilon = \tau(\epsilon) = \sigma(\epsilon)\}$.

Un elemento qualsiasi di LN è della forma:

$$\epsilon = a_0 + a_1\sigma + a_2\sigma^2 + a_3\tau + a_4\sigma\tau + a_5\sigma^2\tau$$

Agendo con τ otteniamo:

$$\tau(\epsilon) = \tau(a_0) + \tau(a_2)\sigma + \tau(a_1)\sigma^2 + \tau(a_3)\tau + \tau(a_5)\sigma\tau + \tau(a_4)\sigma^2\tau$$

Mentre l'azione di σ è:

$$\sigma(\epsilon) = \sigma(a_0) + \sigma(a_1)\sigma + \sigma(a_2)\sigma^2 + \sigma(a_4)\tau + \sigma(a_5)\sigma\tau + \sigma(a_3)\sigma^2\tau$$

Se vogliamo quindi che ϵ sia in $(LN)^{\lambda(G)}$ dobbiamo avere che $\epsilon = a_0 + a_1\sigma + \tau(a_1)\sigma^2 + a_3\tau + \sigma^2(a_3)\sigma\tau + \sigma(a_3)\sigma^2\tau$ con $a_0 \in k,\ a_1 \in L^{<\sigma>},\ a_3 \in L^{<\tau>}$.

Otteniamo allora che: $H \cong k \times L^{<\sigma>} \times L^{<\tau>}$ come $k-$algebre.

4.2 Estensioni di grado piccolo

Se il grado dell'estensione è basso, poichè il teorema 3.3.1 ci chiede di studiare il gruppo di permutazioni di n elementi dove n è il grado dell'estensione, siamo allora in grado di studiare il problema con facilità.

Proposizione 4.2.1. *Sia L/k un'estensione di campi separabile di grado minore o uguale a quattro. Allora L/k ammette almeno una struttura Hopf-Galois.*

Dimostrazione. Come al solito chiameremo con E la chiusura normale di L/k, $G = Gal(E/k)$ e $G' = Gal(E/L)$. Cerchiamo un sottogruppo regolare N di $Perm(G/G')$ normalizzato da $\lambda(G)$.

Se L/k è normale allora il problema è già stato risolto più in generale nella sezione precedente, basta ad esempio prendere $N = \rho(G)$, siamo quindi interessati solo al caso in cui $L \neq E$. In particolare dobbiamo quindi solo considerare il caso di estensioni di grado tre o quattro.

Se $[L : k] = 3$, necessariamente $G \cong S_3$ e quindi per cardinalità $\lambda(G)$ coincide con $Perm(G/G')$. In questo caso è sufficiente prendere allora $N = A_3$ cioè l'insieme dei tre cicli.

Se $[L : k] = 4$ invece abbiamo che G può essere isomorfo a tre gruppi diversi, esaminiamo ciascun caso separatamente.

- $G \cong D_4$: basta prendere un sottogruppo di indice 2 di $\lambda(G)$.
- $G \cong A_4$: si prende $N = V_4$, il gruppo di Klein. Esso agisce transitivamente in $Perm(G/G')$ ed è normale in A_4, essendolo in tutto S_4.
- $G \cong S_4$: si prende lo stesso gruppo del caso precedente.

□

La proposizione precedente ci fa sospettare che quattro sia il grado massimo per cui ogni estensione di quel grado sia Hopf-Galois, e ciò in effetti è vero, faremo infatti ora vedere un esempio di un'estensione di grado cinque che non ammette nessuna struttura Hopf-Galois.

Esempio 4.2.2. Sia L/k un'estensione di grado 5 e supponiamo che il gruppo di Galois G della sua chiusura normale E/k sia tutto S_5. Un esempio di questo tipo si può costruire facilmente ad esempio prendendo $k = \mathbb{Q}$ ed un polinomio di grado cinque su $\mathbb{Q}$ irriducibile ma dotato di esattamente due radici complesse. Se si prende una sola radice allora l'estensione ha grado cinque ma si vede facilmente che il suo campo di spezzamento è invece tutto S_5.

Vogliamo fare vedere che tali estensioni non ammettono struttura Hopf-Galois, ma ciò è facile, infatti abbiamo che $\lambda(G)$ per cardinalità deve coincidere con $Perm(X)$ essendo λ iniettiva. Cerchiamo quindi sottogruppi regolari e normali di S_5. Ma l'unico sottogruppo normale di S_5 non banale è A_5 che non può però essere regolare di nuovo guardando ad esempio la cardinalità.

Avendo visto la proposizione e l'esempio e ricordandoci il teorema che richiede che un certo sottogruppo venga normalizzato da un altro in S_n viene spontaneo supporre che se il grado della chiusura di Galois della nostra estensione è molto più grande del grado dell'estensione allora non avremo nessuna struttura Hopf-Galois. Cerchiamo di caratterizzare meglio questa frase, limitandoci però a trovare delle disuguaglianze molto lasche che con un po' più di fatica potrebbero essere migliorate.

Prendiamo quindi come al solito un'estensione separabile L/k di grado n e sia E la sua chiusura normale con gruppo di Galois G, ci chiediamo quanto può essere grande al massimo il grado di E/k. Identifichiamo $\lambda(G)$ con G e $Perm(X)$ con S_n, se esistesse una struttura Hopf-Galois avremmo quindi che N è normalizzato da G il che implica $\#G \leq \#Cent_{S_n}(N)\#Aut(N)$. Ma $\#Cent_{S_n}(N) = n$ come si vede facilmente usando il fatto che N è regolare, ed altrettando facilmente si vede che N è generato da al più $[log_2 n]$ elementi, quindi $\#Aut(N) \leq n^{[log_2 n]}$.

Otteniamo quindi che se abbiamo una struttura Hopf-Galois allora necessariamente $\#G \leq n \cdot n^{[log_2 n]}$.

Usando questa disuguaglianza o anche, più facilmente, sapendo che A_n è semplice per $n \geq 5$, otteniamo anche la seguente proposizione:

Proposizione 4.2.3. *Se $G \cong S_n$ o $G \cong A_n$ per $n \geq 5$ allora L/k non ammette nessuna struttura Hopf-Galois, dove n è il grado dell'estensione.*

4.3 Estensione con due strutture H-Galois distinte

Applichiamo ora il teorema per trovare tutte le strutture di Hopf-Galois dell'estensione $L = \mathbb{Q}(\sqrt[4]{2})$ su $k = \mathbb{Q}$. Dato che $\sqrt[4]{2}$ ha come polinomio minimo $x^4 - 2$ otteniamo che la chiusura normale sarà il campo $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Notiamo inoltre

immediatamente che $[E : k] = 8$ e $[E : L] = 2$. Se inoltre consideriamo σ tale che $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ e $\sigma(i) = i$ e τ tale che $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$ e $\tau(i) = -i$. Tali mappe possono essere estese su tutta E e lasciano chiaramente k fisso, sono quindi elementi di $G = Gal(E/k)$. Ma esse generano un gruppo diedrale di otto elementi, per cardinalità quindi: $G =< \sigma, \tau >$. Infatti σ ha ordine quattro mentre τ ha ordine due e $\tau\sigma = \sigma^3\tau$. Detto invece $G' = Gal(E/L)$ esso è chiaramente il sottogruppo di G generato da τ.

X sarà quindi un insieme di quattro elementi e dei suoi rappresentanti saranno: $\{\bar{e}, \bar{\sigma}, \bar{\sigma^2}, \bar{\sigma^3}\}$. Identificheremo questi elementi con 1, 2, 3, 4 e il gruppo $Perm(X)$ con S_4. Ricordandoci l'immersione di G in $Perm(X)$ tramite la mappa λ otteniamo immediatamente che $\sigma \to (1234)$ e $\tau \to (24)$. Chiamerò anche questo gruppo con G intendendolo immerso in S_4 e chiamerò σ e τ gli elementi corrispondenti. Per il teorema dobbiamo quindi cercare i sottogruppi regolari di S_4 normalizzati da G. La condizione che il sottogruppo sia regolare però è molto forte, infatti i gruppi di ordine 4 sono o ciclici (e allora sono chiaramente regolari) oppure sono isomorfi a $\mathbb{Z}/2 \times \mathbb{Z}/2$ ma si vede subito che l'unico fatto in questo modo e regolare dentro S_4 è quello che non contiene trasposizioni, ovvero $M =< (13)(24), (12)(34) >$. Fatta questa osservazione si vede facilmente che i gruppi che ci interessano sono solo due e sono:

$N =< (1234) >=< \sigma >$ e $M =< (13)(24), (12)(34) >=< \sigma^2, \sigma\tau >$. Vogliamo trovare nei due casi la Hopf-algebra corrispondente.

4.3.1 Caso N

Per il teorema sappiamo che $H = (EN)^G$ dove la struttura di Hopf-algebra di EN è nota. Chiaramente mi basta verificare sui generatori di G per vedere cosa otteniamo. Un elemento qualsiasi di EN sarà della forma $x = a_0 + a_1\sigma + a_2\sigma^2 + a_3\sigma^3$ con $a_i \in E$ per $i = 0, 1, 2, 3$. Vediamo quindi cosa succede facendo agire σ dove l'azione su N è per coniugio. Chiaramente lascia gli elementi di N invariati quindi: $\sigma(x) = \sigma(a_0) + \sigma(a_1)\sigma + \sigma(a_2)\sigma^2 + \sigma(a_3)\sigma^3$. Affinchè $\sigma(x) = x$ devo quindi avere che $a_i \in E^{<\sigma>} = \mathbb{Q}(i)$.

Abbiamo quindi operato una prima riduzione ed adesso abbiamo che $H = (\mathbb{Q}(i)N)^{<\tau>}$. Scriviamo come prima un elemento di $\mathbb{Q}(i)N$ come $x = a_0 + a_1\sigma + a_2\sigma^2 + a_3\sigma^3$ dove ora però gli a_i sono in $\mathbb{Q}(i)$. $\tau(x) = \tau(a_0) + \tau(a_3)\sigma + \tau(a_2)\sigma^2 + \tau(a_1)\sigma^3$. Otteniamo quindi che $a_0, a_2 \in \mathbb{Q}$ e $a_3 = \tau(a_1)$ imponendo che $\tau(x) = x$.

Abbiamo quindi trovato H, essa è la Hopf-algebra formata dagli elementi: $\{h_0 + h_1(\sigma + \sigma^3) + h_2\sigma^2 + h_3 i(\sigma - \sigma^3) | h_i \in \mathbb{Q}\ per\ i = 0, 1, 2, 3\}$ e dove le mappe sono quelle ereditate da EN dotato della struttura di Hopf-algebra canonica.

Vogliamo ora scrivere tale Hopf-algebra in maniera più semplice. Chiamiamo quindi l'elemento $(\sigma + \sigma^3)/2 = s$ e l'elemento $(\sigma - \sigma^3)/2i = t$. Sapendo che $\sigma^4 = id$ otteniamo che $2s^2 - 1 = \sigma^2$ quindi con tale morfismo se dotiamo s e t della

struttura di Hopf-algebra derivata da quella di H abbiamo che la mappa scritta è un morfismo di Hopf-algebre tra H e $\mathbb{Q}[s,t]$.

Vogliamo quindi ora trovare il Ker di tale morfismo. Sappiamo che in H $\sigma^4 = id$ ed è l'unica relazione che abbiamo. Il Ker sarà quindi l'ideale dei polinomi in s e t che dopo aver applicato il morfismo sono in (σ^4). Noto subito che ts appartiene a tale ideale. Ora vediamo che $s^2 = (1+\sigma^2)/2$ mentre $t^2 = (1-\sigma^2)/2$. Ma allora anche s^2+t^2-1 appartiene a tale ideale e anche $(2s^2-1)^2-1$ e $(2t^2-1)^2-1$. Se consideriamo l'ideale I generato da questi quattro polinomi esso ha come base di Groebner (con l'ordinamento lessicografico $s > t$) $I = (s^2+t^2-1, st, t^3-t)$. Guardando quindi $\mathbb{Q}[s,t]/I$ esso è uno spazio vettoriale su $\mathbb{Q}$ di dimensione 4 che è la stessa dimensione di H, ne deduciamo quindi che tale ideale non è solo contenuto nel Ker ma è il Ker stesso. Abbiamo quindi concluso che $H \cong \mathbb{Q}[s,t]/I$ vogliamo ora per ultima cosa scrivere espressamente come agiscono le mappe che definiscono la Hopf-algebra sui due generatori. Le mappe che definiscono la struttura di algebra sono quelle ovvie. Quelle che definiscono la coalgebra invece abbiamo detto che derivano da quelle di H vista come sottocoalgebra di EN. Quindi:

$$
\begin{aligned}
&s \otimes s = (\sigma+\sigma^3)/2 \otimes (\sigma+\sigma^3)/2 = 1/4(\sigma\otimes\sigma + \sigma\otimes\sigma^3 + \sigma^3\otimes\sigma + \sigma^3\otimes\sigma^3)\\
&s \otimes t = (\sigma+\sigma^3)/2 \otimes (\sigma-\sigma^3)/2i = 1/4i(\sigma\otimes\sigma - \sigma\otimes\sigma^3 + \sigma^3\otimes\sigma - \sigma^3\otimes\sigma^3)\\
&t \otimes s = (\sigma-\sigma^3)/2i \otimes (\sigma+\sigma^3)/2 = 1/4i(\sigma\otimes\sigma + \sigma\otimes\sigma^3 - \sigma^3\otimes\sigma - \sigma^3\otimes\sigma^3)\\
&t \otimes t = (\sigma-\sigma^3)/2i \otimes (\sigma-\sigma^3)/2i = -1/4(\sigma\otimes\sigma - \sigma\otimes\sigma^3 - \sigma^3\otimes\sigma + \sigma^3\otimes\sigma^3)\\
&\Delta(s) = \Delta(\sigma+\sigma^3)/2 = 1/2(\Delta(\sigma)+\Delta(\sigma^3)) = 1/2(\sigma\otimes\sigma + \sigma^3\otimes\sigma^3) = s\otimes s - t\otimes t\\
&\Delta(t) = \Delta(\sigma-\sigma^3)/2i = 1/2i(\Delta(\sigma)-\Delta(\sigma^3)) = 1/2i(\sigma\otimes\sigma - \sigma^3\otimes\sigma^3) = s\otimes t + t\otimes s\\
&\epsilon(s) = \epsilon(\sigma+\sigma^3)/2 = 1/2(\epsilon(\sigma)+\epsilon(\sigma^3)) = 1/2(1+1) = 1\\
&\epsilon(t) = \epsilon(\sigma-\sigma^3)/2i = 1/2i(\epsilon(\sigma)-\epsilon(\sigma^3)) = 0\\
&S(s) = S(\sigma+\sigma^3)/2 = 1/2(S(\sigma)+S(\sigma^3)) = 1/2(\sigma^3+\sigma) = s\\
&S(t) = S(\sigma-\sigma^3)/2i = 1/2i(S(\sigma)-S(\sigma^3)) = 1/2i(\sigma^3-\sigma) = -t
\end{aligned}
$$

4.3.2 Caso M

Come nel caso precedente abbiamo che $H = EM^G$ e scriviamo un qualiasi elemento di EM come $x = a_0 + a_1\sigma^2 + a_2\sigma\tau + a_3\sigma^3\tau$ con $a_i \in E$ $\forall i \in \{0,1,2,3\}$. Notiamo che sia τ che σ agendo per coniugio sugli elementi di M lasciano l'identità e σ^2 invariati mentre mandano $\sigma\tau$ in $\sigma^3\tau$ e viceversa. Quindi se cerchiamo gli elementi

che vengono lasciati fissi da G abbiamo che:

$$\sigma(a_0) = \tau(a_0) = a_0$$
$$\sigma(a_1) = \tau(a_1) = a_1$$
$$\sigma(a_2) = \tau(a_2) = a_3$$
$$\sigma(a_3) = \tau(a_3) = a_2$$

Da cui otteniamo che $a_0, a_1 \in \mathbb{Q}$ mentre $a_2, a_3 \in E^M = \mathbb{Q}(\sqrt{-2})$ perchè $a_2 = \sigma^2(a_2) = \tau\sigma(a_2)$ e similmente per a_3.

Abbiamo allora ottenuto che $H = \{h_0 + h_1(\sigma\tau + \sigma^3\tau) + h_2\sigma^2 + h_3\sqrt{-2}(\sigma\tau - \sigma^3\tau)\}$ dove $h_i \in \mathbb{Q}$ per ogni i.

Come prima vogliamo scriverla in maniera più semplice consideriamo quindi il morfismo che manda a in $(\sigma\tau + \sigma^3\tau)/2$ e b in $\sqrt{-2}/2(\sigma\tau - \sigma^3\tau)$ che come prima diventa un morfismo di Hopf-algebre se diamo a $\mathbb{Q}[a, b]$ la struttura di Hopf-algebra derivata da quella di H. Inoltre sempre come prima è suriettivo infatti $2a^2 - 1 = 1/2((\sigma\tau)^2 + (\sigma^3\tau)^2 + 2\sigma\tau\sigma^3\tau) = 1/2(1 + 1 + 2\sigma^2) - 1 = \sigma^2$.

Svolgendo i conti si ottiene che il Ker è $J = (b^2 - 2a^2 + 2, ba, a^3 - a)$ mentre la struttura di Hopf-algebra è:

$a \otimes a = (\sigma\tau + \sigma^3\tau)/2 \otimes (\sigma\tau + \sigma^3\tau)/2 = 1/4(\sigma\tau \otimes \sigma\tau + \sigma\tau \otimes \sigma^3\tau + \sigma^3\tau \otimes \sigma\tau + \sigma^3\tau \otimes \sigma^3\tau)$
$a \otimes b = \sqrt{-2}/4(\sigma\tau \otimes \sigma\tau - \sigma\tau \otimes \sigma^3\tau + \sigma^3\tau \otimes \sigma\tau - \sigma^3\tau \otimes \sigma^3\tau)$
$b \otimes a = \sqrt{-2}/4(\sigma\tau \otimes \sigma\tau + \sigma\tau \otimes \sigma^3\tau - \sigma^3\tau \otimes \sigma\tau - \sigma^3\tau \otimes \sigma^3\tau)$
$b \otimes b = -1/2(\sigma\tau \otimes \sigma\tau - \sigma\tau \otimes \sigma^3\tau - \sigma^3\tau \otimes \sigma\tau + \sigma^3\tau \otimes \sigma^3\tau)$
$\Delta(a) = \Delta(\sigma\tau + \sigma^3\tau)/2 = (\sigma\tau \otimes \sigma\tau + \sigma^3\tau \otimes \sigma^3\tau)/2 = a \otimes a - 1/2b \otimes b$
$\Delta(b) = \Delta(\sqrt{-2}/2(\sigma\tau - \sigma^3\tau)) = \sqrt{-2}/2(\sigma\tau \otimes \sigma\tau - \sigma^3\tau \otimes \sigma^3\tau) = a \otimes b + b \otimes a$
$\epsilon(a) = \epsilon(\sigma\tau + \sigma^3\tau)/2 = (\epsilon(\sigma\tau) + \epsilon(\sigma^3\tau))/2 = (1 + 1)/2 = 1$
$\epsilon(b) = \epsilon(\sqrt{-2}/2(\sigma\tau - \sigma^3\tau)) = \sqrt{-2}/2(\epsilon(\sigma\tau) - \epsilon(\sigma^3\tau)) = \sqrt{-2}/2(1 - 1) = 0$
$S(a) = S(\sigma\tau + \sigma^3\tau)/2 = (S(\sigma\tau) + S(\sigma^3\tau))/2 = (\sigma\tau + \sigma^3\tau)/2 = a$
$S(b) = S(\sqrt{-2}/2(\sigma\tau - \sigma^3\tau)) = \sqrt{-2}/2(S(\sigma\tau) - S(\sigma^3\tau)) = \sqrt{-2}/2(\sigma\tau - \sigma^3\tau) = b$

Capitolo 5

Ulteriori risultati

In questo ultimo capitolo presenteremo ulteriori risultati sull'argomento dovuti a vari autori. Lo scopo sarà quello di dare una panoramica di quello che si è ottenuto finora nello studio delle estensioni Hopf-Galois. Necessariamente molte dimostrazioni verranno omesse, sarà possibile comunque trovarle in [2], [3] o [5].

5.1 Risultati di Byott

Una delle difficoltà principali che presenta l'utilizzo del teorema 3.3.1 è che il gruppo S_n non è facile da studiare per n grande, presentando moltissimi sottogruppi regolari. Risulta quindi utile cercare di invertire la relazione tra i gruppi N e G. Il lavoro più importante a tal proposito si deve a Byott ed è quello di cui discuteremo in questa sezione.

Partiamo per prima cosa dall'introdurre gli strumenti e le notazioni che useremo in questa sezione. Supponiamo quindi, come in tutto il resto del testo che L/k sia un'estensione di campi finita e separabile e siano E, G, G', X sempre le solite strutture. Se N è un sottogruppo regolare di $Perm(X)$ segue dalla definizione di sottogruppo regolare che la mappa $b : N \to X$ definita da:

$$b(\eta) = \eta([e])$$

dove $[e]$ è la classe dell'identità in G/G' è biettiva. Induce quindi un isomorfismo $\varphi : Perm(X) \to Perm(N)$ dove, dato $\pi \in Perm(X)$ vale:

$$\varphi(\pi) = b^{-1}\pi b$$

Ricordandoci i risultati della sezione 4.1 abbiamo che N può essere immerso in $Perm(N)$ in due modi diversi tramite le mappe che avevamo chiamato λ e ρ. Ma essendo N anche un sottogruppo di $Perm(X)$, esisterà anche una terza immersione, ovvero $\varphi(N)$, essa tuttavia non è dissimile dalle precedenti, vale infatti:

Proposizione 5.1.1. $\varphi(N) = \lambda(N)$.

Dimostrazione. Siano infatti $\mu, \eta \in N$, vale allora che:

$$\varphi(\eta)(\mu) = b^{-1}\eta b(\mu) = b^{-1}(\eta \circ \mu([e])) = \eta \circ \mu = \lambda(\eta)(\mu)$$

□

Inoltre anche $\lambda(G)$ sarà mappata tramite φ in un certo gruppo G_0 in $Perm(X)$ e se $\lambda(G)$ normalizzava N seguirà che G_0 normalizza $\lambda(N)$ in $Perm(N)$. Introduciamo ora una definizione:

Definizione 5.1.2. *L'olomorfo* di N, indicato con $Hol(N)$, è il gruppo dei normalizzatori di $\lambda(N)$ in $Perm(N)$.

Quello che vedremo è che cercare sottogruppi regolari N di $Perm(X)$ normalizzati da $\lambda(G)$ è equivalente a cercare immersioni di G dentro $Hol(N)$. Quest'ultimo però è molto più piccolo di $Perm(X)$, e quindi più facile da descrivere. Faremo inoltre vedere che una volta data l'immersione sarà facile trovare l'Hopf-algebra corrispondente.

Iniziamo quindi a dimostrare un lemma preparatorio ed il teorema principale che ci dà la corrispondenza tra i due insiemi considerati.

Lemma 5.1.3. $Hol(N) = \rho(N) \rtimes Aut(N)$

Dimostrazione. Facciamo per prima cosa vedere che sia $\rho(N)$ che $Aut(N)$ sono sottogruppi di $Hol(N)$. Per $\rho(N)$ questo è ovvio perchè abbiamo già fatto vedere nella sezione 4.1 che centralizza $\lambda(N)$. Prendiamo ora $\gamma \in Aut(N)$ e $\eta, \mu \in N$, abbiamo che:

$$(\gamma\lambda(\eta))(\mu) = \gamma(\eta\mu) = \gamma(\eta)\gamma(\mu) = (\lambda(\gamma(\eta))\gamma)(\mu)$$

da cui $\gamma\lambda(\eta) = \lambda(\gamma(\eta))\gamma$, e quindi $\gamma\lambda(\eta)\gamma^{-1} = \lambda(\gamma(\eta))$ da cui $Aut(N)$ normalizza $\lambda(N)$ ed è quindi incluso in $Hol(N)$.

Dimostriamo ora che $Aut(N) \cap \rho(N) = \{1\} \in Perm(N)$, infatti $Aut(N)$ fissa e, l'identità di N, mentre abbiamo visto che $\rho(N)$ è un sottogruppo regolare, il che in particolare implica che lo stabilizzatore di ogni elemento è banale.

Inoltre, dati come sopra γ, η, μ abbiamo che

$$\gamma\rho(\eta)(\mu) = \gamma(\mu\eta^{-1}) = \gamma(\mu)\gamma(\eta)^{-1} = \rho(\gamma(\eta))(\gamma(\mu))$$

da cui otteniamo che $\gamma\rho(\eta)\gamma^{-1} = \rho(\gamma(\eta))$ e quindi che $\rho(N) \rtimes Aut(N)$ è un sottogruppo di $Perm(X)$ contenuto in $Hol(N)$.

Resta da dimostrare l'inclusione inversa, prendiamo quindi $\pi \in Hol(N)$. Allora per definizione di $Hol(N)$ vale che dato $\eta \in N$ esiste una mappa $\gamma : N \to N$ tale

che $\pi\lambda(\eta)\pi^{-1} = \lambda(\gamma(\eta))$. Si vede immediatamente che la mappa γ così definita è un automorfismo di N, allora:

$$\begin{aligned}\pi(\eta) = \pi\lambda(\eta)(e) = (\lambda(\gamma(\eta))\pi)(e) = \lambda(\gamma(\eta))\pi(e) = \\ = \gamma(\eta)\pi(e) = (\rho(\pi(e)^{-1})\gamma)(\eta)\end{aligned}$$

Quindi $Hol(N) \subseteq \rho(N) \rtimes Aut(N)$.

□

Teorema 5.1.4. *Siano $G' \subseteq G$ gruppi finiti, $X = G/G'$ ed N un gruppo astratto di ordine $|X|$. Esiste allora una biezione tra i due seguenti insiemi:*

$\Theta = \{\alpha : N \to Perm(X)$ *omomorfismo iniettivo tale che* $\alpha(N)$ *sia regolare*$\}$
$\Gamma = \{\beta : G \to Perm(N)$ *omomorfismo iniettivo tale che* $\beta(G')$ *sia lo stabilizzatore di* e_N, *l'identità di* $N\}$

Sotto questa biezione, se $\alpha, \alpha' \in \Theta$ corrispondono a $\beta, \beta' \in \Gamma$ rispettivamente, allora $\alpha(N) = \alpha'(N)$ se e solo se $\beta(G)$ e $\beta'(G)$ sono coniugati tramite un elemento di $Aut(N)$. Inoltre $\alpha(N)$ è normalizzato da $\lambda(G) \subseteq Perm(X)$ se e solo se $\beta(G)$ è contenuto in $Hol(N)$.

Dimostrazione. Sia $\alpha \in \Theta$ vogliamo fargli corrispondere un elemento $\beta \in \Gamma$. Per far questo notiamo che dato che $\alpha : N \to Perm(X)$ è un'immersione regolare allora $X = \alpha(N)[e]$ dove e è l'identità in G. α induce allora una biezione a tra N e X data da $a(\eta) = \alpha(\eta)([e])$. Questa mappa induce a sua volta per coniugio un isomorfismo

$$C(a) : Perm(N) \to Perm(X)$$

dato da $C(a)(\pi) = a\pi a^{-1}$ per ogni $\pi \in Perm(N)$.

Per rendere chiara la notazione indicheremo da qui in avanti con $\lambda_X : G \to Perm(X)$ e con $\lambda_N : N \to Perm(N)$ le due mappe di traslazione a sinistra.

Se ora componiamo $C(a)^{-1}$ con λ_X otteniamo un'immersione di G dentro $Perm(N)$, chiameremo tale elemento β e vogliamo mostrare che è in Γ. L'unica cosa da dimostrare è che $\beta(G')$ stabilizza e_N, ma scrivendo esplicitamente la mappa abbiamo che, $\sigma \in G$:

$$(C(a)^{-1}\lambda_X(\sigma))(e_N) = (a^{-1}\lambda_X(\sigma)a)(e_N)$$

Ma quest'ultimo è uguale a e_N se e solo se $\lambda_X(\sigma)(a(e_N)) = a(e_N)$. Per come abbiamo definito a vale che $a(e_N) = [e]$ e per definizione di λ_X vale $\lambda_X(\sigma)[e] = [\sigma]$. Quindi σ stabilizza e_N se e solo se $[\sigma] = [e]$ cioè se e solo se $\sigma \in G'$. Abbiamo quindi dimostrato che $\beta \in \Gamma$. Chiamiamo la mappa trovata $\phi : \Theta \to \Gamma$. Dove come già detto $\phi(\alpha) = C(a)^{-1}\lambda_X$.

Verifichiamo ora la seguente uguaglianza che ci sarà utile più avanti: $C(a)^{-1}\alpha = \lambda_N$. Infatti, dati $\eta, \mu \in N$ vale che:

$$\begin{aligned}(C(a)^{-1}\alpha(\eta))(\mu) = (a^{-1}\alpha(\eta)a)(\mu) = (a^{-1}\alpha(\eta))(\alpha(\mu)[e]) = \\ = a^{-1}(\alpha(\eta\mu)[e]) = \eta\mu = \lambda_N(\eta)(\mu)\end{aligned}$$

Cerchiamo adesso una mappa ψ che sia l'inversa di ϕ. Prendiamo quindi un elemento $\beta \in \Gamma$, esso induce una biezione $b : X \to N$ data da $\beta([\sigma]) = \beta(\sigma)(e_N)$ per $\sigma \in G$. Tale mappa è una biezione ed è ben definita perchè abbiamo richiesto che $\beta(G')$ sia lo stabilizzatore di e_N. Come prima quindi tramite coniugio otteniamo una mappa $C(b) : Perm(X) \to Perm(N)$ che è un isomorfismo. Vorremmo dimostrare che definendo

$$\psi(\beta) = C(b)^{-1}\lambda_N$$

otteniamo che ψ e la mappa inversa di ϕ ed avremmo così la prima parte del teorema. Il fatto che $\psi(\beta) \in \Theta$ è ovvio quindi bisogna solo verificare che la composizione delle due mappe sia l'identità.

Sia quindi data $\alpha \in \Theta$ e sia $\beta = \phi(\alpha)$. Vediamo com'è definita b:

$$b([\sigma]) = \beta(\sigma)(e_N) = (C(a)^{-1}\lambda_X(\sigma))(e_N) = (a^{-1}\lambda_X(\sigma)a)(e_N) = a^{-1}[\sigma]$$

Allora $\psi(\beta) = C(b)^{-1}\lambda_N = C(a)\lambda_N = \alpha$ dove l'ultima uguaglianza è stata verificata sopra. Similmente si fa la composizione opposta.

Dimostriamo ora i due punti succesivi. Notiamo che $\alpha(N) = \alpha'(N)$ se e solo se detto $\gamma : \alpha^{-1}\alpha : N \to N$ esso è un auomorfismo di N. In particolare avremo che $C(a') = C(a)\gamma$. Ricordandoci quindi la definizione di ϕ avremo che:

$$\phi(\alpha') = C(a')^{-1}\lambda_X = \gamma^{-1}C(a)^{-1}\lambda_X = \gamma^{-1}\phi(\alpha)$$

Cioè β, β' sono coniugati rispetto ad un elemento di $Aut(N)$.

Supponiamo invece che $\alpha(N)$ sia normalizzato da $\lambda_X(G)$ e sia $\beta = \phi(\alpha)$. Dobbiamo dimostrare che $\beta(G)$ normalizza $\lambda_N(N)$, cioè che, dati $\sigma \in G$ e $\eta \in N$ vale che:

$$\beta(\sigma)\lambda_N(\eta)\beta(\sigma)^{-1} \in \lambda_N(N)$$

Si tratta di una semplice verifica, infatti (useremo $C(a)^{-1}\alpha = \lambda_N$):

$$\begin{aligned}\beta(\sigma)\lambda_N(\eta)\beta(\sigma)^{-1} = C(a)^{-1}(\lambda_X(\sigma))\lambda_N(\eta)C(a)^{-1}(\lambda_X(\sigma^{-1})) = \\ = a^{-1}\lambda_X(\sigma)aa^{-1}\alpha(\eta)aa^{-1}\lambda_X(\sigma^{-1})a = \\ = C(a)^{-1}(\lambda_X(\sigma)\alpha(\eta)\lambda_X(\sigma^{-1}))\end{aligned}$$

Per ipotesi però $\lambda_X(\sigma)\alpha(\eta)\lambda_X(\sigma^{-1}) \in \alpha(N)$ quindi usando di nuovo $C(a)^{-1}\alpha = \lambda_N$ abbiamo la tesi.

□

Il teorema appena dimostrato ci permette di avere un modo per contare le strutture Hopf-Galois di una certa estensione separabile L/k in maniera relativamente facile e di scrivere espressamente l'Hopf-algebra corrispondente come si può dedurre dalle due seguenti proposizioni.

Proposizione 5.1.5. *Sia L/k un'estensione finita e separabile e siano E, G, G' come prima. Sia $\mathcal{S}$ l'insieme delle classi di isomorfismo di gruppi N con cardinalità pari a $|G/G'|$. Sia $\mathcal{G}_N$ l'insieme delle classi di equivalenza di immersioni regolari β di G in $Hol(N)$ tali che $\beta(G')$ sia lo stabilizzatore di e_N. Sia infine $e(G,N)$ la cardinalità di $\mathcal{G}_N$ quozientato per la relazione di equivalenza data dal coniugio per elementi di $Aut(N) \subseteq Hol(N)$. Allora il numero di strutture Hopf-Galois su L/k è $s(G,G') = \sum_{\{N\}\in\mathcal{S}} e(G,N)$.*

Dimostrazione. Si tratta semplicemente di mettere insieme il teorema 3.3.1 e il teorema 5.1.4. Per il teorema 3.3.1 il numero di strutture Hopf-Galois è in corrispondenza biunivoca con i sottogruppi regolari N di $Perm(X)$ normalizzati da $\lambda(G)$. Ma quest'ultimi, per il teorema 5.1.4 sono in corrispondenza biunivoca con le classi di equivalenza delle immersioni di G in $Hol(N)$ quozientate per il coniugio tramite elementi di $Aut(N)$. □

Proposizione 5.1.6. *Sia L/k un'estensione finita e separabile, utilizzando le notazioni di cui sopra, sia $\alpha(N)$un'immersione regolare di un gruppo astratto N dentro $Perm(X)$ normalizzata da $\lambda(G)$ e sia $\beta : G \to Hol(N)$ l'omomorfismo corrispondente secondo il teorema 5.1.4. Sia inoltre $\beta_2 : G \to Aut(N)$ β seguito dalla mappa canonica tra $Hol(N)$ e $Aut(N)$. Allora l'Hopf-Galois struttura su L/k corrispondente a $\alpha(N)$ è data dalla Hopf-algebra $H = (EN)^G$ dove G agisce su E tramite l'azione di Galois e su N tramite β_2.*

Dimostrazione. Dalla dimostrazione del teorema 3.3.1 avevamo già notato che si ricavava che $H = (E\alpha(N))^{\lambda(G)}$ dove $\lambda(G)$ agiva su $\alpha(N)$ per coniugio.

Nella dimostrazione del teorema 5.1.4 abbiamo definito la mappa $C(a)$, siamo ora interessati alla sue inversa, $C(a)^{-1} : Perm(X) \to Perm(N)$ la quale soddisfa $\lambda(\eta) = C(a)^{-1}(\alpha(\eta))$ per $\eta \in N$. Quindi $C(a)^{-1}$ mappa in maniera isomorfa $\alpha(N)$ in $\lambda(N)$.

Abbiamo inoltre definito la mappa $\beta : G \to Hol(N)$ corrispondente ad α come $\beta(\sigma) = C(a)^{-1}(\lambda(\sigma))$ per $\sigma \in G$. L'azione di $\lambda(G)$ su $\alpha(N)$ tramite $C(a)^-1$ passa quindi ad un'azione di $\beta(G)$ su $\lambda(N)$, infatti:

$$C(a)^{-1}(\lambda(\sigma)\alpha(\eta)\lambda(\sigma^{-1})) = C(a)^{-1}(\lambda(\sigma))C(a)^{-1}(\alpha(\eta))C(a)^{-1}(\lambda(\sigma^{-1})) = \beta(\sigma)\lambda(\eta)\beta(\sigma^{-1})$$

da cui $H \cong (E\lambda(N))^{\beta(G)}$.

Usando ora il lemma 5.1.3 possiamo scriverci $\beta(\sigma) = \rho(\mu)\delta$ per $\mu \in N$ e $\delta \in Aut(N)$ e segue che $\beta_2(\sigma) = \delta$. Dato ora $\theta \in N$:

$$\begin{aligned}\beta(\sigma)\lambda(\eta)\beta(\sigma^{-1})(\theta) &= (\rho(\mu)\delta\lambda(\eta)(\rho(\mu)\delta)^{-1})(\theta) = (\rho(\mu)\delta\lambda(\eta)\delta^{-1}\rho(\mu^{-1}))(\theta) = \\ &= (\rho(\mu)\delta\lambda(\eta))(\delta^{-1}(\theta\mu)) = \delta(\eta\delta^{-1}(\theta\mu))\mu^{-1} = \delta(\eta)(\theta)\end{aligned}$$

Quindi, per $\sigma \in G$, $\beta(\sigma)$ agisce su $\lambda(N)$ come $\beta_2(\sigma)$ e perciò $H \cong (EN)^G$.

□

5.2 Casi particolari di calcolo delle Hopf-strutture

Un altro utilizzo del teorema 5.1.4 è per trovare le strutture Hopf-Galois di estensioni che hanno un grado particolare. Presenteremo vari teoremi che permettono di contare le strutture in vari casi. Tuttavia lo studio del caso generale di quante strutture ci siano su una data estensione rimane ancora in gran parte ignoto. Per motivi di spazio molte dimostrazioni verranno omesse o solo accennate, si potranno comunque trovare in [2].

Iniziamo a considerare il caso più semplice ovvero di estensioni di grado un numero primo. In questo caso è abbastanza facile dire se esistono o meno strutture Hopf-Galois.

Proposizione 5.2.1. *Sia L/k un'estensione di campi separabile di grado primo. Allora L/k è Hopf-Galois se e solo se $G = Gal(E/k)$ è risolubile, dove E è la chiusura normale di L/k.*

Dimostrazione. Supponiamo prima che L/k sia Hopf-Galois. Esiste quindi un sottogruppo regolare N di $Perm(G/G')$. Per il lemma 5.1.3, essendo N un sottogruppo di ordine p primo allora è ciclico, quindi $Hol(N) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ che è un gruppo risolubile. Per il teorema 5.1.4 esiste allora un'immersione β di G in $Hol(N)$, quindi G essendo sottogruppo di un gruppo risolubile è risolubile.

Vediamo ora l'altra implicazione. Essendo l'estensione di grado p primo abbiamo che $L = k[a_1] \cong k[x]/(f(x))$ dove $f(x)$ è un polinomio irriducibile di grado p e con radici $a_1, \ldots, a_p$ in E. G è un sottogruppo del gruppo delle permutazioni delle radici, inoltre per un teorema della teoria di Galois classica, se G è risolubile allora è isomorfo ad un sottogruppo transitivo di F_p dove:

$$F_p = \{\pi_{r,s} | 0 \leq r, s < p,\ r \neq 0\} \tag{5.2.1}$$

dove $\pi_{r,s}(a_i) = a_{ri+s}$ intendendo il pedice modulo p. Si vede facilmente che $F_p \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ il quale è a sua volta isomorfo a $Hol(N)$. Quindi il fatto che G sia risolubile implica che esiste una sua immersione in $Hol(N)$ che usando di nuovo il teorema 5.1.4 ci porta a concludere che L/k ammette almeno una struttura Hopf-Galois. □

Rimanendo sempre nel caso in cui il grado è una potenza di un primo riusciamo a dire anche diverse altre cose. Consideriamo prima il caso in cui l'estensione sia di Galois classica. Siamo allora in grado di dire esattamente quante strutture diverse abbiamo nel caso di estensioni cicliche.

Teorema 5.2.2. *Sia L/k un'estensione di Galois ciclica di grado p^n. Allora esistono esattamente p^{n-1} strutture Hopf-Galois.*

Nel caso in cui l'estensione non sia normale ma sia pura siamo comunque in grado di contare le strutture. Per estensione pura di grado p^n intendiamo che $L = k[\omega]$ con $\omega^{p^n} \in k$. Supponiamo inoltre che k contenga una radice primitiva p^r-esima dell'unita con $r > 0$ e L non contenga nessuna radice $p^{r+1}-$esima. In questo caso, detto ζ una radice p^n-esima dell'unità abbiamo che $k(\zeta)/k$ è un'estensione di Galois di grado p^{n-r} ed inoltre la chiusura normale di L/k sarà $E = k(\omega, \zeta)$.

Teorema 5.2.3. *Nelle ipotesi precedenti, se $r < n$ allora ci sono esattamente p^r strutture Hopf-Galois su L/k.*

Cambiamo ora completamente punto di vista e torniamo a guardare estensioni di Galois classiche. In questo caso abbiamo che $G' = \{e\}$, quindi riutilizzando le notazioni del teorema 5.1.4 per avere un conto parziale delle strutture Hopf-Galois possiamo limitarci a studiare il numero $e(G, G)$ dove G è il gruppo di Galois. Tale numero risulterà particolarmente facile da calcolare in alcuni casi particolari. Ci soffermiamo in particolare a studiare il caso in cui il gruppo di Galois è semplice e non abeliano oppure il gruppo simmetrico S_n.

Teorema 5.2.4. *Sia A un gruppo semplice non abeliano. Allora $e(A, A) = 2$.*

Teorema 5.2.5. *Sia $S = S_n$ per $n \geq 5$. Allora $e(S, S) =$due volte il numero di permutazioni pari di S il cui ordine divide 2.*

Per terminare la sezione, ci limitiamo ancora al caso di estensioni di Galois classiche ma vogliamo ora vedere quando esse ammettono un'unica struttura. Grazie al lavoro di Byott è possibile caratterizzare in maniera straordinariamente semplice quali sono tali estensioni. La dimostrazione è parecchio lunga ma daremo comunque un'idea dei vari passaggi che sono necessari per ottenere il teorema nella sua forma finale.

Definizione 5.2.6. Un numero g è detto di *Burnside* se $(g, \phi(g)) = 1$.

Teorema 5.2.7 (Teorema di unicità di Byott)**.** *Un'estensione L/k di Galois classica ha un'unica struttura Hopf-Galois (che sarà quella data da kG) se e solo se il grado dell'estensione è un numero di Burnside.*

Dimostrazione. Iniziamo con il dimostrare l'implicazione che se il grado dell'estensione è un numero di Burnside allora esiste un'unica struttura Hopf-Galois. Ci risulterà utile il seguente lemma:

Lemma 5.2.8. *Se G è un gruppo e $|G|$ è un numero di Burnside, allora G è ciclico.*

Usando il lemma quindi, e sapendo che $|N| = |G|$ allora anche tutti i sottogruppi regolari N di $Perm(G)$ sono ciclici e quindi isomorfi a G. Quindi $Hol(N) \cong Hol(G)$, usando il teorema 5.1.4 il numero di strutture Hpf-Galois è uguale al numero di immersioni regolari di G dentro $Hol(G)$ modulo coniugio tramite $Aut(G)$. Detto ora $|G| = g$ dato che G è ciclico abbiamo che $G \cong \mathbb{Z}/g\mathbb{Z}$ e $Aut(G) \cong (\mathbb{Z}/g\mathbb{Z})^*$ ed essendo g un numero di Burnside $(g, |Aut(G)|) = 1$.

Detta ora $\pi : Hol(G) \to Aut(G)$ la proiezione ovvia, abbiamo per il lemma 5.1.3 che $Ker(\pi) = \rho(G)$. Inoltre se $\beta : G \to Hol(G)$ è una qualunque immersione per cardinalità $\pi\beta(G) = \{e\}$. Cioè ogni immersione β è equivalente a ρ modulo il coniugio per $Aut(G)$, abbiamo quindi una delle due implicazioni.

Daremo ora solo un'idea della dimostrazione dell'altra che è notevolmente più complessa. Ovvero dobbiamo dimostrare che se g non è un numero di Burnside allora L/k ammette almeno una struttura Hopf-Galois non classica.

Abbiamo già visto nella sezione 4.1 che questo è vero per le estensioni non abeliane, quindi in questa trattazione possiamo limitarci a supporre G abeliano.

Supponiamo ora che $G = G_1 \times G_2$ e siano N_1, N_1' sottogruppi regolari e distinti di $Perm(G_1)$ normalizzati da $\lambda(G_1)$, e sia N_2 un sottogruppo regolare di $Perm(G_2)$ normalizzato da $\lambda(G_2)$. Ma allora, siccome $Perm(G_1) \times Perm(G_2) \subseteq Perm(G)$ e $\lambda(G_1) \times \lambda(G_2) = \lambda(G)$, abbiamo che $N_1 \times N_2$ e $N_1' \times N_2$ ci danno due strutture Hopf-Galois distinte. Quindi per dire che G ha più di una struttura Hopf-Galois è sufficiente dirlo per un suo sottogruppo.

Utilizzando ora il teorema di struttura è facile ricavare il seguente lemma:

Lemma 5.2.9. *Se G è un gruppo abeliano con g numero non di Burnside allora G ha un sottogruppo di una di queste forme:*

- $G_1 = \mathbb{Z}/p^e\mathbb{Z}$,
- $G_1 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$,
- $G_1 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ *con* $q|p-1$.

Per concludere la dimostrazione del teorema è quindi sufficiente far vedere che in tutti e tre i casi del lemma precedente si riescono a trovare almeno due sottogruppi regolari distinti di $Perm(G_1)$.

□

5.3 Il teorema di corrispondenza

Uno dei teoremi principali della teoria di Galois classica è il teorema di corrispondenza che nel caso di estensioni finite afferma che esiste una corrispondenza biunivoca tra i sottogruppi del gruppo di Galois e le sottoestensioni del campo. Questo teorema ammette varie generalizzazioni nel caso delle estensioni Hopf-Galois, di cui daremo l'enunciato ma non la dimostrazione in questa sezione. Il primo risultato e dal quale si riescono a dedurre in maniera non troppo complicata gli altri afferma che una delle due frecce della corrispondenza è sempre rispettata.

Teorema 5.3.1. *Data un'estensione L/k $H-$Hopf-Galois, la mappa che associa ad ogni sottoHopf-algebra di H la sottoestensione di L che rimane fissata da lei è iniettiva.*

Tale teorema viene dimostrato in [5], mentre i teoremi che enunceremo successivamente nella sezione si possono tutti trovare dimostrati in [3].

Vorremmo tuttavia ritrovare la forma classica del teorema di corrispondenza, ovvero che tale mappa sia anche suriettiva. Ciò non vale in generale ma in alcuni casi sì, diamo quindi una definizione per caratterizzare un particolare tipo di estensioni Hopf-Galois.

Definizione 5.3.2. Un'estensione L/k è detta un'*estensione di Galois quasi classica* se esiste un sottogruppo regolare N di $Perm(X)$ normalizzato da $\lambda(G)$ e contenuto in $\lambda(G)$.

Dove le notazioni nella definizione sono le stesse usate nei capitoli precedenti.

Possiamo notare che tutti gli esempi di estensioni Hopf-Galois dati nel capitolo 4 sono in realtà casi di estensioni di Galois quasi classiche, verrebbe quindi da chiedersi se tutte le estensioni Hopf-Galois sono quasi classiche, ma questo è falso. Un controesempio non è tuttavia così immediato da costruire ma con un po' di lavoro si riesce a dimostrare che l'estensione $L = \mathbb{Q}(\sqrt{-2}, \sqrt[16]{2})$ su $k = \mathbb{Q}(\sqrt{-2})$ è Hopf-Galois ma non quasi classica. Il motivo per cui abbiamo introdotto questo tipo particolare di estensioni è appunto il fatto che il teorema precedente può essere potenziato, ovvero:

Teorema 5.3.3. *Se L/k è un'estensione di Galois quasi classica, allora esiste una Hopf algebra H tale che L/k sia $H-$Galois e la mappa definita nel teorema precedente è sia iniettiva che suriettiva.*

Un ultimo caso che volevamo vedere è quello delle estensioni di Galois classiche. Abbiamo visto nel capitolo precedente che possono esistere più strutture Hopf-Galois su tali estensioni, in particolare abbiamo visto che se il gruppo è non abeliano ne esistono due canoniche. Una è quella che deriva dalla struttura di Galois classica e per la quale quindi il teorema di corrispondenza vale nella sua forma

più forte. Ci chiediamo ora se l'altra dia origine a tipi particolari di sottoestensioni ed in effetti è proprio così.

Teorema 5.3.4. *Ogni estensioni di Galois L/k possiede una struttura $H-$Galois tale che valga la seguente variante del teorema di corrispondenza. Esiste una corrispondenza biunivoca tra le sottoHopf-algebre di H e i campi intermedi normali di L/k*

Segue inoltre dalla dimostrazione del teorema, che però non vedremo, che l'Hopf-algebra è proprio quella che avevamo trovato in generale nel capitolo precedente.

Questi risultati vogliono dare una panoramica ulteriore su quanto è stato studiato in questi anni sull'estensioni Hopf-Galois e far notare che il fatto che la struttura non sia univoca, a differenza del caso classico, porta ad avere una certa libertà di scelta di volta in volta su quale sia la struttura migliore da utilizzare.

Bibliografia

[1] Moss E. Sweedler, *Hopf Algebras*, W. A. Benjamin Inc., 1969

[2] Lindsay N. Childs, *Taming Wild Extension: Hopf Algebras and Local Galois Module Theory*, American Mathematical Society, 2000

[3] Cornelius Greither e Bobo Pareigis, *Hopf Galois Theory for Separable Field Extensions*, Journal of Algebra vol. 106, 1987, 239-258

[4] Charles W. Curtis e Irving Reiner, *Methods of representation theory vol. 1* Wiley-Interscience publication, 1981

[5] S. U. Chase e M. E. Sweedler *Hopf Algebras and Galois Theory* Lecture Notes in Mathematics vol. 97 Springer-Verlag