UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Triennale in Matematica

Teoria di Galois secondo Grothendieck

.

ELABORATO SCRITTO DI
Emiliano Ambrosi Maria
Matricola 792212

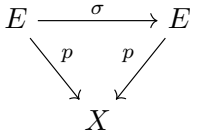
SOTTO LA GUIDA DI
Prof. Fabrizio Andreatta

Anno Accademico 2013/2014

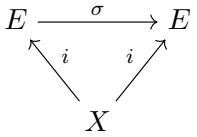
Introduzione

Dietro ogni astrazione si nasconde l'intuizione di una Totalità.
E.Severino

Nello studio dei rivestimenti di uno spazio topologico X sufficientemente regolare si scopre che il gruppo fondamentale dello spazio è isomorfo al gruppo degli automorfismi del rivestimento universale E. Usando una notazione di tipo diagrammatico abbiamo che, a meno di isomorfismo, $\pi_1(X, x)$ non è altro che il gruppo degli automorfismi σ di E che rendono commutativo il seguente diagramma:



D'altro canto il gruppo di Galois di un'estensione di campi $X \subseteq E$ non è altro che il gruppo degli automorfismi di E che rendono commutativo il seguente diagramma:



Riformulando in questi termini relazionali un teorema e una definizione ci si rende facilmente conto della presenza di un'analogia fra le due costruzioni, che non si ferma qui. Andando un po' più a fondo si scopre che i rivestimenti intermedi si ottengono come quozienti del rivestimento universale mediante un'azione di un'unico sottogruppo del gruppo degli automorfismi mentre le estensioni intermedie si ottengono come campi fissati da un unico sottogruppo del gruppo di Galois. Lo scopo di questo elaborato è mettere in luce e formalizzare queste analogie, mostrando che entrambe le costruzioni sono, in un certo senso, casi particolari di una teoria più generale.
Tra i vari problemi che si riscontrano nel tentativo di farlo, uno dei primi è sicuramente di linguaggio. Infatti le due costruzioni sono relative ad

oggetti molto diversi, da una parte abbiamo oggetti geometrici e dall'altra oggetti algebrici, da una parte abbiamo azioni sulla fibra di morfismi e dall'altra azioni sulle radici di polinomi. E' necessario quindi un linguaggio che non guardi all'interno degli oggetti ma si curi solo di studiare le relazioni reciproche tra questi. La scelta dunque non può che cadere nel linguaggio delle categorie, che già molte volte ha permesso di riassumere con una definizione unica costruzioni profondamente diverse. Per convincersi di questo è sufficiente pensare alla nozione *"locale"* di funtore rappresentabile e alla sua controparte *"globale"* di aggiunzione. Queste infatti racchiudono la gran parte delle costruzioni *"canoniche"* della matematica, a partire dall'oggetto libero fino ad arrivare al prodotto tensore, in un'unica definizione, permettendo di vedere tutte le costruzioni come casi particolari di una costruzione più generale. Il linguaggio categoriale si rivelerà quello giusto anche in questo caso in quanto permetterà di definire le categorie Galoisiane, che da una parte sono l'ambiente giusto per generalizzare il gruppo fondamentale e dall'altro si caratterizzano come categorie su cui questo agisce.
La possibilità di utilizzare il linguaggio categoriale mette in luce anche un altro aspetto: le costruzioni del gruppo fondamentale e del gruppo di Galois si possono recuperare a partire dalle relazioni reciproche degli oggetti. In questo si vede un riflesso del lemma di Yoneda: tutte le proprietà interessanti di un oggetto sono determinate dagli omomorfismi da e verso questo.
Per quanto riguarda l'organizzazione dell'elaborato, questo è diviso in tre capitoli.
Nel primo svilupperemo il linguaggio e la tecnica necessaria per i capitoli successivi, in particolare parleremo di limiti, colimiti, gruppi profiniti e dimostreremo una serie di lemmi che semplificheranno il lavoro in seguito.
Nel secondo definiremo le categorie Galoisiane e mostreremo il teorema principale dell'elaborato che le caratterizza come categorie sui quali oggetti è definita un'azione continua di un gruppo profinito.
Nel terzo mostreremo come e in che senso le categorie Galoisiane siano una generalizzazione sia del gruppo fondamentale che del gruppo di Galois.

Indice

Capitolo 1

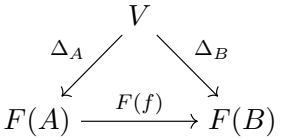
Preliminari algebrici

In questa sezione svilupperemo la teoria che ci servirà in seguito, sia da un punto di vista astratto sia attraverso alcuni esempi. In particolare daremo le definizioni di limite e colimite nel linguaggio della teoria delle categorie e ne mostreremo la realizzazione pratica in alcuni casi concreti. Poi dimostreremo una serie di teoremi e lemmi che ci saranno utili in seguito. Infine costruiremo i gruppi profiniti e ne studieremo alcune proprietà.

1.1 Limiti e colimiti

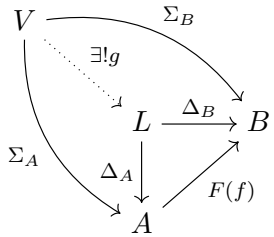
Definizione 1.1 (Cono per un funtore)**.** Sia $F : C \to D$ un funtore. Un cono per F è una coppia (V, Δ) dove $V \in Ob(D)$ e Δ è una trasformazione naturale tra F e il funtore costante in V.

Equivalentemente un cono è un oggetto V di D con una collezione di mappe $(\Delta_A)_{A \in Ob(C)}$ tale che ogni diagramma come il seguente commuti.



$\forall A, B \in Ob(C)$ e $\forall f \in Hom_C(A, B)$

Definizione 1.2 (Limite per un funtore)**.** Sia $F : C \to D$ un funtore. Un limite per F è un cono (L, Δ) terminale, ovvero tale che per ogni altro cono (V, Σ) $\exists!$ $g : V \to L$ tale che $\Delta_A \circ g = \Sigma_A$ e $\Delta_B \circ g = \Sigma_B$.



$\forall A, B \in Ob(C)$ e $\forall f \in Hom_C(A, B)$

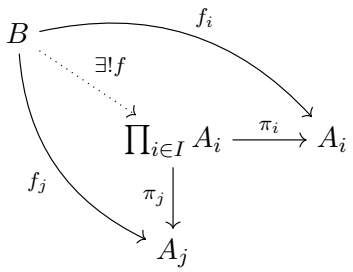
Osservazione 1.
Spesso diremo, con abuso di linguaggio, che L è il limite per il funtore, dimenticandoci della trasformazione naturale e lo indicheremo con LimF

Osservazione 2.
Non necessariamente esiste il limite per un funtore. Più avanti vedremo alcune condizioni necessarie e sufficienti affinché questo avvenga

Consideriamo ora una serie di limiti particolarmente utili e importanti.

Definizione 1.3 (Prodotto)**.** Sia I una categoria discreta. Un prodotto è un limite per un funtore da I a C.

Equivalentemente il prodotto di una famiglia $(A_i)_{i\in I}$ di oggetti di C, che indicheremo con $\prod_{i\in I} A_i$, è un oggetto, con un famiglia di mappe π_i, tale che $\forall B$ e $\forall\ (f_i \in Hom_C(B, A_i))_{i\in I}$ $\exists!$ f:$B \to \prod_{i\in I} A_i$ tale che $f_i = \pi_i \circ f\ \forall i$



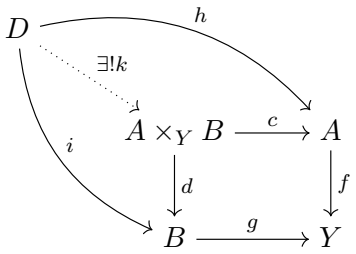
Osservazione 3. Dalla proprietà universale del prodotto segue che se $f, g \in Hom(A, \prod_{i\in I} A_i)$ sono tali che $\pi_i \circ f = \pi_i \circ g\ \forall i \in I$ allora $f = g$, ovvero che una mappa verso il prodotto è unicamente determinata dalle proiezioni.

Definizione 1.4 (Oggetto terminale)**.** Un oggetto terminale di una categoria C, che indicheremo con 1, è il limite per l'unico funtore dalla categoria vuota a C.

Equivalentemente un oggetto terminale 1, è tale che $\forall A \in Ob(C)$ $\exists!$ $f : A \to 1$

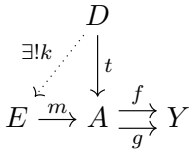
Definizione 1.5 (Pullback)**.** Siano $f \in Hom_C(A, Y)$ e $g \in Hom_C(B, Y)$. Sia D la categoria come nel disegno $\bullet \xrightarrow{a} \bullet \xleftarrow{b} \bullet$. Il pull back di f e g è il limite per l'unico funtore che manda a in f e b in g.

Equivalentemente il pullback di f e g, , che indicheremo con $A \times_Y B$, è un oggetto con due mappe c,d tali che $f \circ c = g \circ d$, e tale che $\forall D$ e $\forall h \in Hom_C(D, A)$ $\forall i \in Hom_C(D, B)$ tali che $f \circ h = g \circ i$, $\exists!$ $k \in Hom_C(D, A \times_Y B)$ che rende commutativo in ogni sua parte il seguente diagramma:



Definizione 1.6 (Equalizzatore)**.** Siano $f, g \in Hom_C(A, Y)$. Sia D la categoria come nel disegno $\bullet \underset{b}{\overset{a}{\rightrightarrows}} \bullet$. L'equalizzatore di f e g è il limite per l'unico funtore che manda a in f e b in g.

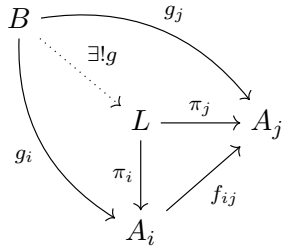
Equivalentemente l'equalizzatore di f,g è un oggetto E, con un mappa m, tale che $m \circ f = m \circ g$ e tale che $\forall D$ e $\forall t \in Hom_C(D, A)$ tale che $t \circ f = t \circ g$, $\exists!\ k \in Hom_C(E, Y)$ tale che $m \circ k = t$.



Osservazione 4. Dalla proprietà universale dell'equalizzatore segue che la mappa m è un monomorfismo.

Definizione 1.7 (Limite inverso)**.** Sia I un insieme diretto, ovvero un insieme parzialmente ordinato tale che per ogni $i, j \in I$ esiste k tale che $i \leq k$ e $j \leq k$. Guardiamo I come una categoria dell'ordine. Un limite inverso è un limite per un funtore A da I^{op} a C.

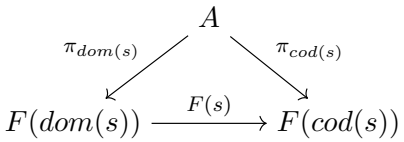
Equivalentemente il limite inverso di una collezione di oggetti $(A_i)_{i \in I}$ di una categoria e di una collezione di mappe $(f_{ij} : A_i \to A_j)_{i,j \in I; i \geq j}$ tali che $f_{ii} = Id_{A_i}\ \forall i$ e $f_{ik} = f_{jk} \circ f_{ij}\ \forall i, j, k \in I$ con $\forall i \geq j \geq k$ è un oggetto, che indicheremo con $Lim_I A$, con una collezione mappe $\pi_i \in Hom(Lim, A_i)$ tali che $\forall i, j \in I\ \forall i \geq j$ si abbia $f_{ij} \circ \pi_i = \pi_j$ e tale che per ogni altro oggetto B e per ogni altra collezione di mappe $g_i \in Hom(B, A_i)$ con la stessa proprietà $\exists! g$ che renda commutativo il seguente diagramma.



Definizione 1.8 (Completezza)**.** Una categoria C si dice (finitamente) completa , se per ogni categoria D piccola (finita) e ogni funtore $D \to C$ ammette limite.

Proposizione 1.1.1 (Completezza via prodotti ed equalizzatori)**.**
Una categoria C è (finitamente) completa $\iff$ ha prodotti (finiti) ed equalizzatori.

Dimostrazione. $\implies$ per definizione
$\impliedby$ Sia C una categoria con prodotti ed equalizzatori e $F : I \to C$ un funtore. Consideriamo il prodotto $A = \prod_{i \in Ob(I)} F(i)$, con le mappe canoniche π_i, e $B = \prod_{s \in Arrow(I)} D(cod(s))$. Per ogni $s \in Arrow(I)$ definiamo
$\psi_s = \pi_{cod(s)} : A \to D(cod(s))$
$\varphi_s = F(s) \circ \pi_{dom(s)} : A \to D(cod(s))$



Per la proprietà universale di B otteniamo una coppia di frecce $A \underset{\varphi}{\overset{\psi}{\rightrightarrows}} B$
Sia ora (L,l) l'equalizzatore di queste due frecce. Vogliamo mostrare che $(L, (l_i = \pi_i \circ l)_{i \in OB(I)})$ è il limite per il funtore F. Che sia un cono è chiaro (in quanto l,essendo un equalizzatore fa commutare tutti i diagrammi come quello sopra), rimane da verificare la proprietà universale. Questa però discende dalle proprietà universali di A e di L. Infatti dato un oggetto S e una famiglia di mappe $s_i \in Hom_C(S, F(i))$ tali che $s_j = F(f) \circ s_i$, per la proprietà universale di A esiste un unico morfismo $s : S \to A$ tale che $s_i = \pi_i \circ s$. Ma L è l'equalizzatore e $\psi \circ s = \varphi \circ s$ in quanto $\pi_i \circ \psi \circ s = \pi_i \circ \varphi \circ s$ e quindi esiste un morfismo k: $S \to L$, che fa commutare tutto. L'unicità segue dal fatto che l è mono. □

Proposizione 1.1.2. *Set è completa.*

Dimostrazione. Il prodotto cartesiano usuale è il prodotto nella categoria Set. Infatti se S è un insieme e $s_i \in Hom_{Set}(S, A_i)\ \forall i \in I$ possiamo definire un'unica mappa s tale $\pi \circ s = s_i$:
$s : S \to \prod_{i \in I} A_i;\ x \mapsto (s_i(x))_{i \in I}$.

Inoltre date $A \underset{g}{\overset{f}{\rightrightarrows}} B$ esiste il loro equalizzatore Infatti sia $X = \{a \in A | f(a) = g(a)\}$ e i l'inclusione di X in A. Allora (X,i) è l'equalizzatore di f,g. Infatti $g \circ i = f \circ i$ e se C è un altro insieme con una mappa e con la stessa proprietà si ha che $Ime \subset X$ e quindi possiamo definire $k : C \to X$

$c \mapsto e(c)$. Questa mappa è tale che $i \circ k = e$ e l'unicità segue dall'iniettività di i. La tesi segue quindi dal teorema precedente □

Osservazione 5.
Vediamo quindi che il limite per un funtore verso Set, è il più grande sottoinsieme del prodotto di cartesiano delle immagini che fa commutare tutti i triangoli immagine del funtore. In questo senso possiamo pensare ai limiti come la miglior soluzione al problema di far commutare una serie di diagrammi.

Proposizione 1.1.3 (Limiti e rappresentabilità)**.**
Se C è una categoria localmente piccola, un funtore $F : I \to C$ ammette limite $\iff$ il funtore $G : C^{op} \to Set$ $A \mapsto Lim(Hom_c(A, F(-)))$ è rappresentabile.

Dimostrazione. $\implies$ Sia $(L, (l_i)_{i\in I})$ il limite del funtore F. Per il teorema precedente sia che $G(X) = \{(f_i) \in \prod_{i\in I} Hom(X, F(i)) \mid F(s) \circ f_i = f_j \ \forall s : i \to j\}$. Conserviamo quindi $\alpha_X : Hom(X, L) \to G(X)$ $\alpha_X(f) := (l_i \circ f)$. Questa risulta essere una biezione $\forall X$, per la proprietà universale di L ed è naturale in quanto se $g : X \leftarrow Y$ allora $\forall f \in Hom(X, L))$ si ha che $g \circ \alpha_X(f) = (l_i \circ f \circ g)_{i\in I} = \alpha_Y(f \circ g)$
$\impliedby$ Sia L il rappresentante del funtore G e μ la trasformazione naturale tra Hom(-,L) e G. Definiamo quindi $l_i : L \to F(i)$ $l_i = \pi_i \circ \mu_L(1_L)$ dove π_i sono le proiezioni di G(L). Il lemma di Yoneda ci dice che ogni altra collezione di mappe fattorizza tramite l_i in modo unico e per la naturalità di μ si ha che $\forall f : i \to j$ $F(f) \circ l_i = l_j$.

□

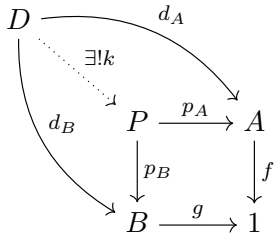
Corollario 1.1.4.
Un limite se esiste è unico a meno di un'unico isomorfismo ed è quindi univocamente determinato dalla sua proprietà universale.

Osservazione 6. Il prodotto è quindi associativo a meno di un isomorfismo canonico. Infatti si ha che $(A \times B) \times C \approx A \times (B \times C) \approx A \times B \times C$ in quanto soddisfano tutti la stessa proprietà universale. In particolare una categoria ammette prodotti finiti se e solo se ammette il prodotto per ogni coppia di oggetti.

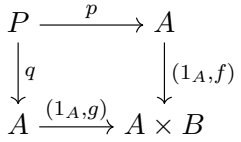
Proposizione 1.1.5 (Completezza via pullback e oggetto terminale)**.**
Una categoria C è finitamente completa $\iff$ ha i pullback è l'oggetto terminale

Dimostrazione. $\implies$ per definizione
$\impliedby$ Mostriamo che C ammette prodotti binari ed equalizzatori. Siano $A, B \in Ob(C)$ e f, g le uniche mappe da loro verso l'oggetto terminale 1 e sia $(P, (p_A, p_B))$ il pullback di f e g. Vogliamo mostrare che P è il prodotto di A e B. Siano allora d_A, d_B due mappe da D a A e B. Si ha che $g \circ d_B = f \circ d_A$, in

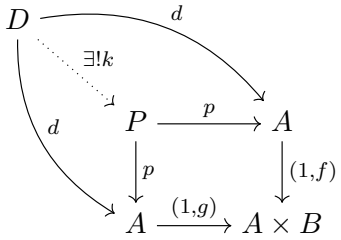
quanto esiste un unico mappa da D a 1. Quindi, per la proprietà universale del pullback esiste unica $k \in Hom(D, P)$ tale che $p_A \circ k = d_A$ e $p_B \circ k = d_B$.



Mostriamo che C ammette equalizzatori. Date f,g come nel diagramma: $A \underset{g}{\overset{f}{\rightrightarrows}} B$ consideriamo il seguente diagramma di pullback.



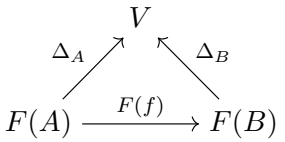
Innanzitutto notiamo che p=q. Infatti $p = \pi_A \circ (1_A, f) \circ p = \pi_A \circ (1_A, g) \circ q = q$. Vogliamo mostrare che (P,p) è l'equalizzatore di f e g. Si ha che $f \circ p = \pi_B \circ (1_A, f) \circ p = \pi_B \circ (1_A, g) \circ p = g \circ p$. Sia ora (D, d) tale che $d \circ f = d \circ g$. Si ha anche che $d \circ (1_A, f) = d \circ (1_A, g)$ e quindi, per la proprietà universale del pullback $\exists! k$ tale che $p \circ k = d$



□

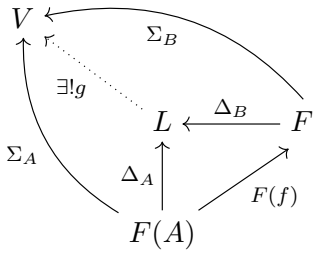
Tutte le costruzioni e teoremi precedenti si posso dualizzare invertendo il verso delle frecce. Vediamo gli esempi più significativi e enunciamo i teoremi, la cui dimostrazione si ottiene per dualità.

Definizione 1.9 (Cocono per un funtore)**.** Sia $F : C \to D$ un funtore. Un cocono per F è una coppia (V, Δ) dove $V \in Ob(D)$ e Δ è una trasformazione naturale tra il funtore costante in V e F.



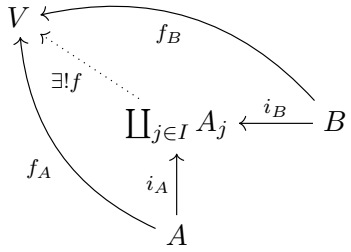
$\forall A, B \in Ob(C)$ e $\forall f \in Hom_C(A, B)$

Definizione 1.10 (Colimite per un funtore)**.** Sia $F : C \to D$ un funtore. Un colimite per F è un cocono (L, Δ) iniziale, ovvero tale che per ogni altro cocono (V, Σ) $\exists!\ g : L \to V$ tale che $\Delta_A \circ g = \Sigma_A$ e $\Delta_B \circ g = \Sigma_B$.



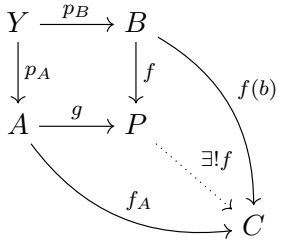
$\forall A, B \in Ob(C)$ e $\forall f \in Hom_C(A, B)$

Definizione 1.11 (Coprodotto)**.** Sia J una categoria discreta. Un coprodotto è un colimite per un funtore da J a C.

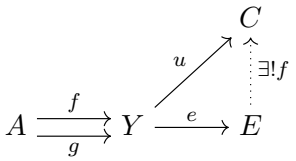


Definizione 1.12 (Oggetto iniziale)**.** Un oggetto iniziale di una categoria C, che indicheremo con 0, è il colimite per l'unico funtore dalla categoria vuota a C.

Definizione 1.13 (Pushout)**.** Siano $f \in Hom_C(Y, A)$ e $g \in Hom_C(Y, B)$. Sia D la categoria come nel disegno. $\bullet \xleftarrow{a} \bullet \xrightarrow{b} \bullet$ Il pushout P di f e g è il colimite per l'unico funtore che manda a in f e b in g.



Definizione 1.14 (Coequalizzatore)**.** Siano $f, g \in Hom_C(A, Y)$. Sia D la categoria come nel disegno. $\bullet \underset{b}{\overset{a}{\rightrightarrows}} \bullet$ Il coequalizzatore E di f e g è il colimite per l'unico funtore che manda a in f e b in g.



Definizione 1.15 (Limite diretto)**.** Sia I un insieme diretto. Guardiamo I come una categoria dell'ordine. Un limite diretto è un colimite per un funtore da I a C.

Definizione 1.16 (Cocompletezza)**.** Una categoria C si dice (finitamente) cocompleta , se per ogni categoria D piccola (e finita)e ogni funtore (con D finita) $D \to C$ ammette colimite.

Proposizione 1.1.6 (Cocompletezza via coprodotti ed coequalizzatori)**.**
Una categoria C è (finitamente) cocompleta $\iff$ ha coprodotti (finiti) ed coequalizzatori.

Proposizione 1.1.7 (Set è cocompleta)**.** *Dimostrazione.* L'unione disgiunta, con le mappe di inclusione, è il coprodotto in Set. Infatti dato X e $f_i \in Hom(A_i, X)$ possiamo definire in modo unico $f \in Hom(\coprod_{i \in I} A_i, X)$ $f(a_i \in A_i) = f_i(a_i)$, tale che $f \circ j_i = f_i$, dove j_i sono le mappe di inclusione. Inoltre data una coppia di mappe $f, g : A \to B$ possiamo definire su B la più piccola relazione di equivalenza tale che $f(a) \approx g(a)\ \forall a \in A$. L'insieme quoziente $B/\approx$, insieme con la proiezione sul quoziente, è il coequalizzatore, per le note proprietà degli insiemi quoziente. □

Proposizione 1.1.8 (Colimiti e rappresentabilità)**.**
Un funtore $F : I \to C$ ammette colimite $\iff$ il funtore $G : C \to Set$ $A \mapsto lim(Hom_C(F(-), A))$ è rappresentabile

Proposizione 1.1.9 (Cocompletezza via pushout e oggetto iniziale)**.**
Una categoria C è finitamente cocompleta $\iff$ ha pushout e l'oggetto iniziale.

1.2 Alcuni lemmi categoriali

Lemma 1.2.1 (Caratterizzazione equivalenze)**.**
Sia F: $C \to D$. F fa parte di un equivalenza di categorie $\iff$ F è pienamente fedele e essenzialmente suriettivo

Dimostrazione. $\Longrightarrow$ Sia G il quasi inverso di F, e $\alpha : 1_C \xrightarrow{\cdot} GF \quad \beta : 1_D \xrightarrow{\cdot} FG$ i due isomorfismi naturali. Per ogni $f : X \to Y$ si ha che $f = (\alpha_Y)^{-1} \circ GF(f) \circ \alpha_X$ Quindi se f e g sono tali che F(f)=f(g) allora $f = (\alpha_Y)^{-1} \circ GF(f) \circ \alpha_X = (\alpha_Y)^{-1} \circ GF(g) \circ \alpha_X = g$. Quindi F è fedele, e analogamente si mostra che G è fedele. Sia $g : F(X) \to F(Y)$. Definiamo $f = (\alpha_Y)^{-1} \circ G(g) \circ \alpha_X$, ma si ha che $(\alpha_Y)^{-1} \circ G(g) \circ \alpha_X = f = (\alpha_Y)^{-1} \circ GF(f) \circ \alpha_X$. Poiché α_X e α_Y sono isomorfismi si ha che $G(g) = GF(f)$ e dato che G è fedele $g = F(f)$. Quindi F è pieno. Se $X \in OB(D)$ allora $FG(X) \simeq X$ e quindi F è essenzialmente suriettivo.

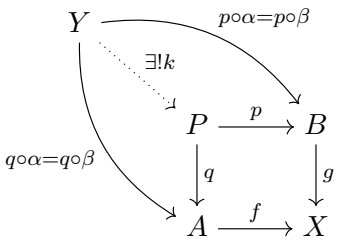
$\Longleftarrow \forall Y \in Ob(D)$ scegliamo $X_Y \in Ob(X)$ tale che $F(X_Y) \simeq Y$ e un isomorfismo $\beta_Y : F(X_Y) \to Y$. Se $f : Y \to Y'$ possiamo considerare $(\mu_{Y'})^{-1} \circ f \circ \mu_Y$ e definire, grazie al fatto che F è pieno e fedele, $G(f) = F^{-1}((\mu_{Y'})^{-1} \circ f \circ \mu_Y)$ Verifichiamo che G è un funtore e che è il quasi inverso di F. $G(Id_Y) = F^{-1}((\mu_Y)^{-1} \circ Id_Y \circ \mu_Y) = F^{-1}(Id_Y) = Id_{X_Y}$ sempre grazie al fatto che è F è un funtore fedele. $G(g \circ f) = F^{-1}((\mu_{Y''})^{-1} \circ g \circ f \circ \mu_Y) = F^{-1}((\mu_{Y''})^{-1} \circ g \circ \mu_{Y'} \circ (\mu_{Y'})^{-1} \circ f \circ \mu_Y) = G(g) \circ G(f)$, ancora grazie al fatto che F è fedele. Le applicazioni μ_Y al variare di Y definisco un isomorfismo naturale da FG al funtore identico su D. Ci rimane da definire un isomorfismo α da GF all'identità su C. Se $X \in Ob(C)$ si ha un isomorfismo $\mu_{F(X)} : FGF(X) \to F(X)$. poiché F è pienamente fedele esiste un isomorfismo α_X tale $F(\alpha_X) = \mu_{F(X)}$. La famiglia di questi α definisce un isomorfismo tra GF e l'identità, la cui naturalità segue da quella di μ e, ancora, dal fatto che F è pieno e fedele. □

Lemma 1.2.2 (I monomorfismi sono stabili per pullback)**.**

$$\begin{array}{ccc} P & \xrightarrow{p} & B \\ \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & X \end{array}$$

Se il quadrato precedente è un quadrato di pullback e f (rispettivamente g) è mono allora p (rispettivamente q) è mono.

Dimostrazione. Siano $\alpha, \beta \in Hom(Y, P)$ tali che $p \circ \alpha = p \circ \beta$. Allora $f \circ q \circ \alpha = g \circ p \circ \alpha = g \circ p \circ \beta = f \circ q \circ \beta$ e quindi, poiché f è mono, $q \circ \alpha = q \circ \beta$. Ma ora sia $p \circ \alpha = p \circ \beta$ sia $q \circ \alpha = q \circ \beta$ sono tali che $f \circ q \circ \alpha = g \circ p \circ \alpha$ e quindi per la proprietà universale del pullback $\exists! k \in Hom(Y, P)$ tale che $p \circ k = p \circ \alpha$ e $q \circ k = q \circ \alpha$. Ma sia α che β hanno questa proprietà e quindi $k = \alpha = \beta$.



□

Lemma 1.2.3 (Caratterizzazione dei monomorfismi tramite pullback)**.**

$$\begin{array}{ccc} A & \xrightarrow{1_A} & A \\ \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle m} \\ A & \xrightarrow{m} & X \end{array}$$

Il quadrato precedente è di pullback $\iff$ *m è mono*

Dimostrazione. $\implies$ se $f, g \in Hom(C, A)$ sono tali che $m \circ f = m \circ g$ allora $m \circ 1_A \circ f = m1_A \circ g$ e quindi, ragionando come nel teorema precedente, per la proprietà universale del pullback si ha che $f = g$
$\impliedby$ se $f, g \in Hom(C, A)$ sono tali che $m \circ f = m \circ g$ si ha che $f = g$ e quindi $\exists! k = f = g$ tale che $1_A \circ f = 1_A \circ g$. □

Lemma 1.2.4. *Se* $F : C \to$ *commuta con i pullback allora manda mono in mono.*

Dimostrazione. Se m è mono, il quadrato del lemma precedente è di pullback. Quindi l'immagine del quadrato tramite F è ancora di pullback, e la tesi segue dal fatto che $F(1_A) = 1_{F(A)}$ e dal lemma precedente.

$$\begin{array}{ccc} F(A) & \xrightarrow{1_{F(A)}} & F(A) \\ \downarrow{\scriptstyle 1_{F(A)}} & & \downarrow{\scriptstyle m} \\ F(A) & \xrightarrow{m} & F(X) \end{array}$$

□

Lemma 1.2.5. $m : X \to Y$ *è mono* $\iff$ *la mappa* $X \times_Y X$ *è un isomorfismo.*

Dimostrazione. Analoga alle precedenti □

Lemma 1.2.6. *Sia I è un insieme diretto,* $F : I \to C$ *è un funtore. Se* $J \subseteq I$ *è cofinale,ovvero* $\forall i \in I$ *esiste* $j \in J$ *tale che* $i \leq j$ *e indichiamo ancora con* $F : J \to C$ *è la restrizione del funtore F a J, allora* $lim_J F \simeq lim_I F$.

Dimostrazione. Dimostriamo che $lim_J F$ soddisfa la stessa proprietà universale di $lim_I F$. Sia $\{g_i\}_{i\in I}$, $g_i : A \to F(i)$, è una famiglia di mappe compatibili con il sistema inverso, dove A è un oggetto di C. Per ogni $i \in I$ esiste $j \in J$ e $f_{ij} : F(i) \to F(j)$ compatibile con le altre mappe del sistema inverso. Quindi considerando $f_{ij} \circ g_i$ otteniamo una famiglia di mappe $\{g_j\}_{j\in J}$ e per la proprietà universale del limite inverso otteniamo la mappa cercata da C a $lim_J F$.

1.3 Gruppi profiniti

Definizione 1.17. Una prebase per uno spazio topologico è una famiglia di aperti tali che le loro intersezioni finite siano una base.

Definizione 1.18. Data una famiglia di spazi topologici $(X_i)_{i\in I}$ definiamo la topologia prodotto sull'insieme $\prod_{i\in I} X_i$ come la più piccola topologia che rende le proiezioni continue.

Osservazione 7. Sicuramente questa topologia esiste, in quanto è l'intersezione di tutte le topologie che rendono le proiezioni continue e questa famiglia è non vuota in quanto almeno la topologia discreta gli appartiene.

Osservazione 8. Equivalentemente si poteva definire questa topologia come quella che ha come prebase aperti della forma $\pi_i^{-1}(U)$ al variare di $i \in I$ e di U tra gli aperti di X_i. La necessità di introdurre la nozione di prebase viene proprio dall'esigenza di definire in un prodotto infinito di spazi topologici una buona topologia. Infatti non si può procedere come nel caso finito, scegliendo come base di $\prod X_i$ gli aperti nella forma $\prod U_i$ con U_i sottoinsieme aperto di X_i in quanto ci sarebbero troppi aperti. Per rendere le proiezioni continue è sufficiente considerare aperti solo prodotti della forma $\prod U_i$ con solo un numero finito di U_i diversi da X_i, in quanto questo basta a garantire che le intersezioni finite di aperti siano aperte. Chiaramente questa definizione coincide con quella usuale di prodotto nel caso di prodotti finiti.

Osservazione 9. Notiamo inoltre che questa costruzione è il prodotto in Top, in quanto eredità la proprietà universale dall'analoga costruzione in Set e in quanto una mappa $Y \to \prod_{i\in I} X_i$ è continua se e solo se sono continue le proiezioni.

Definizione 1.19. Sia GrTop la categoria dei gruppi topologici e I un insieme diretto. Un gruppo profinito è il limite inverso di un funtore $F : I \to GrTop$ tale che F(i) è finito e dotato della topologia discreta.

Lemma 1.3.1. *Ogni F come nella definizione precedente ammette limite.*

Dimostrazione. Prendendo spunto dalla costruzione in Set vogliamo mostrare che L=$\{ (x_i)_{i\in I} \in \prod_{i\in I} F(i)$ tali che $f_{ij}(x_i) = x_j \forall i, j \in I$ con $j \leq i\}$ è il limite inverso. Per farlo notiamo che ci basta dimostrare che è un

sottogruppo del prodotto, in quanto se è così eredita la proprietà universale dalle analoghe costruzioni in Set,Top, Grp. Ma $L = \cap_{i,j}(G_{i,j})$ dove $G_{i,j} = \{(x_k)_{k\in I} \in \prod_{k\in I} F(k)$ tali che $f_{ij}(x_i) = x_j\}$. Ogni $G_{i,j}$ è un sottogruppo del prodotto e quindi L è un sottogruppo in quanto intersezione di sottogruppi. □

Lemma 1.3.2. *Se $G = limG_i$ è un gruppo profinito allora gli aperti nella forma $\pi_i^{-1}(U)$ con U sottoinsieme aperto di G_i formano una base per la topologia di G*

Dimostrazione. Una base per la topologia di $\prod_{i\in I} G_i$ è fatta da intersezioni finite di aperti nella forma $\pi_i^{-1}(U_i)$ con U_i aperto in G_i. Quindi una base per G è fatta da intersezione di aperti della forma $\pi_i^{-1}(U_i)\cap G$. Per mostrare la tesi mostriamo ogni aperto $P = G \cap \pi_{i_1}^{-1}(U_{i_1}) \cap \pi_{i_2}^{-1}(U_{i_2}) \cap ... \cap \pi_{i_n}^{-1}(U_{i_n})$ si scrive come unione di aperti della forma $\pi_i^{-1}(U)$. Se $g = (g_i)_{i\in I} \in P$ poiché I è diretto esiste k tale che $k \geq i_1, ...i_n$ e poiché le f_{ij} sono continue $f_{ki_j}^{-1}(U_{i_j})$ è aperto per ogni $j \in \{1...n\}$. Consideriamo ora l'aperto $U = \cap_{j\in\{1...n\}} f_{ki_j}^{-1}(U_{i_j})$ di G_k e mostriamo che $g \in \pi_k^{-1}(U) \subseteq P$ per ottenere la tesi. $g_k \in U$ in quanto $f_{ki_j}(g_k) = \pi_{i_j}(g) \in U_{i_j}$ per ogni $j \in \{1...n\}$ e quindi $g \in \pi_k^{-1}(U)$. Se $a = (a_i)_{i\in_I} \in \pi_k^{-1}(U)$ allora $a_k = \pi_k(a) \in U$ e quindi $\pi_{i_j}(a) = f_{ki_j} \circ \pi_k(a) \in U_{i_j}$ e quindi $a \in P$. □

Lemma 1.3.3. *Sia G uno spazio topologico compatto e $(C_i)_{i\in I}$ una famiglia di chiusi tale che ogni sua sottofamiglia finita ha intersezione non vuota. Allora $C = \cap_{i\in I} C_i$ è non vuoto.*

Dimostrazione. Definiamo $A_i = G\backslash C_i$. Se per assurdo C fosse vuoto allora $\cup_{i\in I} A_i = \cup_{i\in I} G\backslash C_i = G\backslash \cap_{i\in I} C_i = G$. Quindi gli A_i formano ricoprimento aperto di G e quindi possiamo estrarne un sotto ricoprimento finito $A_{i_1}...A_{i_n}$. Ma quindi $G = \cup A_{i_1} \cup ... \cup A_{i_n} = \cup G\backslash C_{i_1} \cup ... \cup G\backslash C_{i_n} = G\backslash(C_{i_1} \cap ... \cap C_{i_n})$ e di conseguenza $C_{i_1} \cap ... \cap C_{i_n}$ è vuoto contro l'ipotesi. □

Lemma 1.3.4. *Se $G = lim_I G_i$ è un limite inverso di spazi topologici finiti e dotati della topologia discreta allora G è non vuoto.*

Dimostrazione. Definiamo $\forall k \in I$ $L_k = \{(g_i) \in \prod_{i\in I} G_i | g_i = f_{k,i}(g_k) \forall i \leq k \in I\}$ e notiamo che, poiché ogni G_i è di Hausdorff, L_k è chiuso in quanto intersezione di chiusi. Se scegliamo un $g_k \in G_k$ possiamo considerare l'elemento di $g = (g_i)_{i\in I} \in L_k$ tale che $g_i = f_{k,i}(g_k)$ per ogni $i \leq k$ e $g_i \in G_i$ altrimenti. Quindi L_k è non vuoto per ogni k. Dato che I è diretto ogni sottofamiglia finita di $(L_i)_{i\in I}$ ha intersezione non vuota. Inoltre, per il teorema di Tychonoff, $\prod_{i\in I} G_i$ è compatto e $G = \cap_{i\in I} L_i$. La tesi segue allora dal lemma precedente. □

Proposizione 1.3.5. *Se $G = lim_I G_i$ è un gruppo profinito tale che $\forall i \leq j$ $f_{j,i} : G_j \to G_i$ è suriettiva allora $\pi_i : G \to G_i$ è suriettiva $\forall i \in I$*

Dimostrazione. Fissiamo un $i \in I$, un $g_i \in G_i$ e sia $J = \{j \in I | i \leq j\}$. Per ogni $j \in J$ definiamo $Y_j = f_{j,i}^{-1}(g_i)$ e notiamo che sono finiti e dotati della topologia discreta. Per il lemma precedente $lim_J Y_j$ è non vuoto e quindi esiste un $h = (h_j)_{j \in J}$ compatibile con le $f_{i,j}$. Se $k \in I/J$ scegliamo un $j \in J$ tale che $i, k \leq j$. Definiamo quindi $h_k = f_{j,k}(h_j)$ e consideriamo l'elemento $g = (h_i)_{i \in I}$ per ottenere la tesi. □

Definizione 1.20. Se G è un gruppo topologico e E è un G-insieme, diciamo che l'azione di G su E è continua se l'applicazione $G \times E \to E$ è continua una volta che abbiamo dotato E della topologia discreta.

Lemma 1.3.6. *Sia G è un gruppo profinito con un'azione transitiva su E finito. Allora l'azione è continua $\iff \forall e \in E$ $Stab(e)$ è un sottogruppo aperto.*

Dimostrazione. $\Rightarrow$ Detta γ la mappa che definisce l'azione, poiché la topologia su E è quella discreta, $\forall e \in E$ abbiamo che $\gamma^{-1}(e) = \{(g, f) | g \in G, f \in E$ e $g * f = e\}$ è aperto. Poiché E è finito $\gamma^{-1}(e) = \cup_{i \in I, f \in J} U_i \times \{f\}$ con U_i aperti in E e J qualche sottoinsieme di E. Consideriamo un $g \in Stab(e)$ e costruiamo un suo intorno aperto interamente contenuto in $Stab(e)$. Poiché sicuramente $Stab(e) \times \{e\} \subseteq \gamma^{-1}(e)$ esiste un $i \in I$ tale che $\{g\} \times \{e\} \in U_i \times \{e\}$. Se $h \in U_i$ allora $h * e = e$, quindi $h \in Stab(e)$ e di conseguenza $U_i \subseteq Stab(e)$.
$\Leftarrow$ Dobbiamo mostrare che $\forall e \in E$, $\gamma^{-1}(e)$ è aperto e iniziamo a notare che $\forall f \in E$ esiste $h \in G$ tale che $h * f = e$. $(g, f) \in \gamma^{-1}(e)$ se e solo $g * f = e$ se e solo se $g * f = h * f$ se e solo se $h^{-1} g * f = f$ se e solo se $h^{-1} g \in Stab(f)$ se e solo $g \in h^{-1}(Stab(f))$. Quindi $\gamma^{-1}(e)$ è unione di insieme della forma $h^{-1}(Stab(f)) \times \{f\}$ che sono aperti per ipotesi e quindi l'azione è continua. □

Lemma 1.3.7. *Ogni gruppo topologico agisce in modo continuo tramite moltiplicazione su se stesso e sulle sue classi laterali. Inoltre se $N \leq H \leq G$ sono sottogruppi di G, $\frac{G}{H} \simeq \frac{\frac{G}{N}}{\frac{H}{N}}$ come G-insiemi.*

Dimostrazione. E' sufficiente ripetere la dimostrazione del terzo teorema di isomorfismo per gruppi e notare che le biezioni ottenute sono compatibili con l'azione di G di moltiplicazione su i laterali. □

Proposizione 1.3.8. *Se $G = lim_I G_i$ è un gruppo profinito tale che $\forall i \in I$ $\pi_i : G \to G_i$ è suriettiva e $L \leq G$ è un sottogruppo aperto allora $\frac{G}{L} \simeq \frac{G_i}{H}$ come G-insiemi per qualche G_i e qualche $H \leq G_i$*

Dimostrazione. Dimostriamo innanzitutto che esiste k tale che $ker(\pi_k) \subseteq L$. Dato che L è un sottogruppo $1_G \in L$ e dato che è aperto esiste un aperto P di G tale che $1_G \in P \subseteq L$. Poiché una base di aperti per G è fatta da elementi nella forma $\pi_i^{-1}(U_i)$ con U_i aperto in G_i esiste k tale che $1_G \in \pi_k^{-1}(U_k) \subseteq L$. Quindi $ker(\pi_k) = \{g \in G | p_k(g) = 1_{G_k}\} \subseteq \{g \in G | \pi_k(g) \in U_k\} \subseteq L$

Poiché π_k è suriettiva, $\frac{G}{ker(\pi_k)} \simeq G_k$. (La mappa ottenuta è sicuramente un isomorfismo di gruppi, è sicuramente continua ed è chiusa in quanto $\frac{G}{ker(\pi_k)}$ è finito e G_k di Hausdorff). Per il terzo teorema di isomorfismo abbiamo che $\frac{G}{L} \simeq \frac{\frac{G}{ker(\pi_k)}}{\frac{L}{ker(\pi_k)}} \simeq \frac{G_k}{H}$ dove H corrisponde tramite l'isomorfismo tra $\frac{G}{ker(\pi_k)}$ e G_k a $\frac{L}{ker(\pi_k)}$ □

Teorema 1.3.9. *Sia $G = limG_i$ è un gruppo profinito suriettivo e agisce su E in modo continuo e transitivo allora $E \simeq \frac{G_i}{H}$ come G-insieme per qualche G_i e qualche $H \leq G_i$*

Dimostrazione. Poiché l'azione è transitiva e continua, fissato un $e \in E$ Stab(e) è un sottogruppo aperto. Inoltre l'applicazione suriettiva
$\psi_e : G \to E$ $g \mapsto g * e$, dove $g * e$ è l'azione dell'elemento di g su e, definisce per passaggio al quoziente una biezione tra $\frac{G}{Stab(e)}$ ed E. Inoltre G agisce in maniera continua su $\frac{G}{Stab(e)}$ per moltiplicazione e chiaramente la biezione preserva questa azione. Ma $\frac{G}{Stab(e)}$ è isomorfo a $\frac{G_k}{H}$ e quindi la tese segue. □

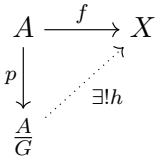
Capitolo 2

Categorie Galoisiane

In questa sezione studieremo e caratterizzeremo l'oggetto centrale di questo elaborato, le categorie Galoisiane. L'obbiettivo sarà quello di dimostrare che data una categoria C dotata di un funtore F verso Sets, soggetta a particolari ipotesi, esiste un gruppo profinito π tale che C è equivalente alla categoria degli insiemi finiti dotati di un'azione continua di π. Potremo a quel punto definire π come il gruppo fondamentale della categoria e nel capitolo successivo vedremo che in un certo senso, questo gruppo è una generalizzazione sia del gruppo di fondamentale di uno spazio topologico sia del gruppo di Galois di un'estensione di campi.
Il processo si articola in tre passi. In primo luogo daremo una forma canonica e maneggevole al funtore F, dimostrando che si scrive come colimite di particolari Hom-set. Il secondo passo consisterà nel costruire π, come limite di particolari gruppi di automorfismi e di mostrare alcune sue proprietà. Infine dimostreremo l'equivalenza di categorie.

2.1 Definizioni ed esempi

Definizione 2.1 (Quoziente per un sottogruppo degli automorfismi)**.** Sia C una categoria, $A \in Ob(C)$ e $G < Aut(A)$. Il quoziente di A per G, è un oggetto $\frac{A}{G}$ con un mappa $p : A \to \frac{A}{G}$ tale che $\forall g \in G$, $p \circ g = p$ dotato della seguente proprietà universale:
$\forall f : A \to X$ tale che $f \circ g = f$ per ogni $g \in G$, $\exists! h : \frac{A}{G} \to X$ tale che $h \circ p = f$.



Osservazione 10. In Set il quoziente $\frac{A}{G}$ è il quoziente di A per la relazione di equivalenza tale che $x \approx y$ se $\exists g \in G$ tale che $x = g(y)$

Esempio 2.1.1. La categoria dei gruppi e degli omomorfismi di gruppi ammette i quozienti per un sottogruppo del gruppo degli automorfismi. Infatti se A è un gruppo e $G \leq Aut(A)$ definiamo $\frac{A}{G}$ come il quoziente di A per il più piccolo sottogruppo normale T che contiene gli elementi della forma $\sigma(a)*a^{-1}$ al variare di $a \in A$ e $\sigma \in G$. Se $f : A \to B$ è tale che $f \circ \sigma = f$ per ogni $\sigma \in G$, si ha che per ogni $a \in A$ $f(\sigma(a)*a^{-1}) = f(\sigma(a))*f(a^{-1}) = f(a)*f(a^{-1}) = 1$ e quindi $T \subseteq Kerf$. Di conseguenza esiste un'unica mappa $\psi : \frac{A}{G} \to B$ tale che $\psi \circ \pi = f$ dove π è la proiezione canonica $A \to \frac{A}{T}$.

Definizione 2.2 (Categoria Galoisiana)**.** Una categoria Galoisiana è una categoria C, con un funtore, detto funtore fondamentale, $F : C \to Sets$, dove Sets è la categoria degli insiemi finiti, con le seguenti proprietà:

1. C ha limiti finiti
2. C ha coprodotti e oggetto iniziale
3. C ammette i quozienti per un sottogruppo del gruppo degli automorfismi
4. ogni freccia f di C ammette una fattorizzazione epi-mono, ovvero esistono m mono, e epi tali che $f = m \circ e$
5. se $m : A \to B$ è mono esiste $Z \in Ob(C)$ tale che $B = A \coprod Z$
6. se $e : A \to B$ è epi allora F(e) è epi
7. F commuta con i limiti, con le somme e con i quozienti
8. F riflette gli isomorfismi, ovvero se $f : A \to B$ è tale che F(f) è un isomorfismo allora f è un isomorfismo.

D'ora in poi C sarà una categoria Galoisiana e F il suo funtore fondamentale

Definizione 2.3 (Sottoggetto)**.** $A \in Ob(C)$ si dice sottoggetto di $B \in Ob(C)$ se esiste $m : A \to B$ mono. Due sottogetti $m : A \to B$, $m' : A' \to B$ sono considerati equivalenti se esiste un isomorfismo $\psi : A \to A'$ tale che $m' \circ \psi = m$

Definizione 2.4 (Oggetti connessi)**.** $A \in Ob(C)$ si dice connesso se non è l'oggetto iniziale e $m : X \to A$ mono implica $X = 0$ o m iso.

Esempio 2.1.2. Ovviamente la categoria Sets è di Galois, e gli oggetti connessi sono solo i singoletti.

Esempio 2.1.3. Se G un gruppo profinito si verifica facilmente che la categoria $G-sets$ è di Galois, con il funtore dimenticante come funtore fondamentale, con le analoghe costruzioni di Sets. Se A è un sottoggetto di B, possiamo identificare A con un sottoinsieme di B chiuso rispetto all'azione di G, quindi con un orbita. Di conseguenza gli oggetti connessi sono gli insiemi su cui G agisce transitivamente.

2.2 F è prorappresentabile

Lemma 2.2.1. *F manda mono in mono*

Dimostrazione. Segue dal lemma 1.2.6 e dal fatto che F commuta con il pullback. □

Lemma 2.2.2. $F(A) = \emptyset \iff A \simeq 0$

Dimostrazione. $\implies$ Se $F(A) = \emptyset$, in particolare $F(A) \simeq \emptyset = F(0)$. Poiché F riflette gli iso si ha $A \simeq 0$
$\impliedby$ per l'assioma 4. □

Osservazione 11. Poiché F commuta con il pullback, con i monomorfismi e ricordando che in Set in pullback di due sottoinsiemi non è altro che la loro intersezione si ha che due sottoggetti Y,Z di X sono gli stessi se e solo F(Y)=F(Z) come sottoinsiemi di F(X).

Proposizione 2.2.3. *Ogni oggetto è il coprodotto di un numero finito di oggetti connessi unici a meno di isomorfismo.*

Dimostrazione. **Esistenza**.
Sia $X \in Ob(C)$. La tesi si dimostra per induzione su n=|F(X)|.
n=1 sia $m : A \to X$ un sottoggetto diverso da 0. Allora F(m) è mono e F(A) è diverso dal vuoto. Quindi |F(A)|=1 e F(m) è iso. Poiché F riflette gli iso m è iso e quindi X è connesso.
n-1 $\Rightarrow$ n Sia $m : A \to X$ un sottoggetto diverso da 0. Allora per l'assioma 5 esiste B tale che $X = A \coprod B$ e quindi, per l'assioma 7, $F(X) = F(A \coprod B) = F(A) \coprod F(B)$. Se $F(B) = \emptyset$ allora A è isomorfo X e quindi X è connesso. Se $F(B) \neq \emptyset$ allora $|F(A)| < |F(X)|$,$|F(B)| < |F(X)|$ e per ipotesi induttiva $A = \coprod_{i \in I} A_i$ e $B = \coprod_{j \in J} B_i$ per I,J finiti e A_i e B_i connessi. Quindi X=$\coprod_{i \in I} A_i \coprod_{j \in J} B_i$
Unicita'.
Siano A_i $i \in I$ e B_j $j \in J$ due famiglie di oggetti connessi tali che X sia isomorfo al coprodotto di entrambi. Fissato un A_i e un $a \in F(A_i)$ si ha che $\exists j \in J$ tale $a \in F(B_j)$. Ma allora il pullback in Set delle mappe di inclusione è non vuoto poiché a gli appartiene. Di conseguenza, poiché il pullback di mono è mono, per la connessione di A_i e B_i si ha che il pullback è isomorfo

sia ad A_i che a B_i che sono quindi isomorfi. Rimane solo da notare che l'isomorfismo, per come è stato costruito, commuta con le inclusioni. □

Lemma 2.2.4. *Sia (A, a) con A connesso e $a \in F(A)$. Allora $\forall X \in Ob(C)$ l'applicazione $\psi^X_{(A,a)} : Hom_C(A, X) \to F(X)$, $f \mapsto Ff(a)$ è iniettiva.*

Dimostrazione. Siano $f, g : A \to X$ tali che Ff(a)=Fg(a) e consideriamo il loro equalizzatore (E,m). Per l'assioma 1 si ha che (F(E),F(m)) è l'equalizzatore di F(f) e F(g). Notiamo che $F(E) \neq \emptyset$ in quanto a appartiene all'immagine di $F(m)$. Quindi E è un sottoggetto non banale di A e per connessione m è un isomorfismo. Quindi f=g. □

Proposizione 2.2.5. *L'insieme I={(A,a) / A connesso, $a \in F(A)$} con la relazione $(B, b) \leq (A, a)$ se $\exists f^A_B \in Hom_C(A, B)$ tale che $F(f^A_B)(a) = b$ è un insieme diretto, ordinato a meno di isomorfismo.*

Dimostrazione. Che I sia parzialmente ordinato è banale, in quanto la riflessività si ottiene considerando la funzione identica, e la transitività considerando la composizione di funzioni. Se $(B, b), (A, a) \in I$ allora per l'assioma 1 posso considerare il prodotto $A \times B$. Si ha che, per l'assioma 7, $F(A \times B) = F(A) \times F(B)$ e quindi consideriamo C, la componente connessa di $A \times B$ tale che $(a, b) \in F(C)$. Si quindi che $(A, a) \leq (C, (a, b))$ con $f^C_A = \pi_A$ la proiezione sul primo fattore e analogamente per (B, b). Se $(B, b) \leq (A, a)$ e $(A, a) \leq (B, b)$ allora esistono f^A_B e f^B_A tali che $F(f^A_B)(a) = b$ e $Ff^B_A(b) = a$. Ma allora $F(f^A_B \circ f^B_A)(b) = b$ e $F(f^B_A \circ f^A_B)(a) = a$, e poiché anche $F(1_B)(b) = b$ e $F(1_A) = A$ dalla connessione di A e B segue che $f^A_B \circ f^B_A = 1_B$ e $f^B_A \circ f^A_B = 1_A$. □

Per ogni $(B, b) \leq (A, a) \in I$ e ogni $X \in Ob(C)$ definiamo

$$\varphi^{(B,b)}_{(A,a)} : Hom_C(B, X) \to Hom_C(A, X)$$
$$\varphi^{(B,b)}_{(A,a)}(f) = f \circ f^A_B.$$

Una $f : X \to Y$ induce una famiglia di applicazioni
$f_A : Hom(A, X) \to Hom(A, Y)$ che rendono il seguente diagramma commutativo per ogni $(A, a) \leq (B, b) \in I$:

$$\begin{array}{ccc} Hom(B,X) & \xrightarrow{f_B = f\circ(-)} & Hom(B,Y) \\ \downarrow{\scriptstyle \varphi^{(B,b)}_{(A,a)}} & & \downarrow{\scriptstyle \varphi^{(B,b)}_{(A,a)}} \\ Hom(A,X) & \xrightarrow{f_A = f\circ(-)} & Hom(B,Y) \end{array}$$

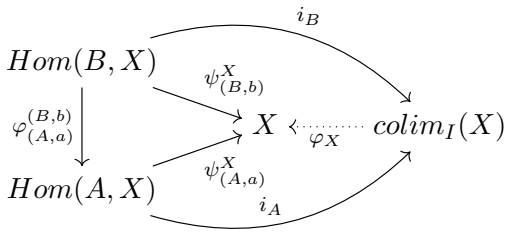
$(f_A \circ i_A)_{(A,a)\in I}$ induce quindi una mappa

$$Colim_I(f) : Colim_I(Hom(A, X)) \to Colim_I(Hom(B, X))$$
$$Colim_I(f)([g]) = [f \circ g]$$

Possiamo quindi definire un funtore $Colim_I : C \to Sets$.

Teorema 2.2.6. *F è naturalmente isomorfo a $Colim_I$*

Dimostrazione. Sia $X \in Ob(C)$. Innanzitutto notiamo che se $(B,b) \leq (A,a)$ e $f \in Hom(B,X)$ allora $\psi^X_{(A,a)} \circ \varphi^{(B,b)}_{(A,a)}(f) = \psi^X_{(A,a)}(f \circ f^A_B) = F(f \circ f^A_B)(a) = F(f(b)) = \psi^X_{(B,b)}$ e quindi per la proprietà universale del limite inverso $\exists! \varphi_X \in Hom(colim_I(X), X)$ che rende commutativo il seguente diagramma.



Esplicitamente $\varphi_X([f]) = Ff(a)$ se $f \in Hom_C(A,X)$. Vogliamo mostrare che φ_X è una biezione ed è naturale al variare di $X \in Ob(C)$.

- φ_X è iniettiva. Infatti poiché l'insieme è diretto, per ogni coppia di classi di equivalenza possiamo scegliere come rappresentanti una coppia di frecce appartenenti allo stesso Hom(C,X) con C connesso. Quindi se f,g sono tali che $\varphi_X([f]) = \varphi_X([g])$ allora F(f(x))=F(g(x)) e la tesi segue dalla connessione di C.

- φ_X è suriettiva. Infatti se $x \in X$ possiamo scegliere la coppia (C,x) dove C è la componente connessa di X tale che F(C) contiene x. Se i è la mappa di inclusione allora $\varphi_X(i) = F(i(x)) = x$.

- φ_X è naturale. Per mostrare che F è naturalmente equivalente a $Colim_I$ è sufficiente notare che il seguente diagramma è commutativo $\forall f : X \to Y$.

$$\begin{array}{ccc} Colim_I(X) & \xrightarrow{\varphi_X} & F(X) \\ \downarrow{\scriptstyle Colim_I(f)} & & \downarrow{\scriptstyle F(f)} \\ Colim_I(X) & \xrightarrow{\varphi_Y} & F(Y) \end{array}$$

  Infatti se $k \in Hom(A,X)$ con $(A,a) \in I$ $F(f) \circ \varphi_X([k]) = F(f) \circ F(k)(a) = F(f \circ k)(a) = \varphi_Y \circ Colim_I(f)(k)$

□

Osservazione 12. Poiché sono proprio le mappe che definiscono il sistema diretto a realizzare l'isomorfismo tra A e B se $(A, a) \leq (B, b)$ e $(B, b) \leq (A, a)$, il limite diretto indicizzato da I è isomorfo al limite indicizzato da una qualunque scelta di un sottoinsieme di I tale che contenga tutte le classi di isomorfismo. Di conseguenza da ora in poi confonderemo I con un suo sottoinsieme che contiene una coppia per ogni classe di isomorfismo, e lo considereremo a tutti gli effetti un insieme ordinato.

2.3 Un gruppo profinito

Definizione 2.5 (Oggetti di Galois)**.** $A \in Ob(C)$ si dice di Galois se è connesso e $\frac{A}{Aut(A)} = 1$

Lemma 2.3.1. *Un oggetto A è di Galois* $\iff$ *L'azione di* $Aut(A)$ *su F(A) è libera e transitiva.*
In questo caso si ha che $|F(A)| = |Aut(A)| = |Hom(A, A)|$

Dimostrazione. Per la connessione di A e quindi l'iniettività della mappa $\psi^X_{(A,a)}$ si ha che $|Aut(A)| \leq |Hom(A, A)| \leq |F(A)|$. Inoltre $\{1\} = F(1) = F(\frac{A}{Aut(A)}) = \frac{F(A)}{Aut(A)}$ e quindi c'è una sola orbita e l'azione è transitiva. In particolare $|F(A)| \leq |Aut(A)|$, quindi $|F(A)| = |Aut(A)|$ e l'azione è anche libera per ragioni di cardinalità. □

Proposizione 2.3.2. *Per ogni X esiste A di Galois tale che* $\varphi^X_{(A,a)} : Hom(A, X) \to F(X)$ *è biettiva* $\forall a \in F(A)$

Dimostrazione. Sia $Y = X^{F(X)}$. Si ha che $F(Y) = F(X)^{F(X)}$ e quindi possiamo considerare l'elemento $a \in F(Y)$ che alla componente x-esima ha l'elemento $x \in F(X)$ Sia ora A la componente connessa di Y tale che $a \in F(A)$. $\varphi^X_{(A,a)}$ è suriettiva in possiamo considerare $\forall x \in F(X)$ la composizione p_x dell'inclusione di A in Y con la proiezione sull'x-esimo fattore:$F(p_x)(a) = x$. Poiché A è connesso abbiamo che $\varphi^X_{(A,a)}$ è iniettiva e quindi biettiva. Inoltre le mappe p_x sono distinte fra loro e sono quindi tutte e sole le mappe da A a X. Ci rimane da mostrare che A è di Galois e lo facciamo mostrando che Aut(A) agisce transitivamente su F(A). Sia $b \in F(A)$. Poiché $\varphi^X_{(A,b)}$ è biettiva e le mappe da A a X sono solo proiezioni si ha che le componenti di b sono gli elementi di x, ognuno una sola volta. Quindi b differisce da a per una permutazione. Possiamo quindi considerare l'automorfismo σ di Y che permuta i fattori, ottenuto ad esempio tramite la proprietà universale scegliendo una diversa indicizzazione. Detta $i : A \to Y$ l'inclusione, consideriamo il seguente diagramma di pullback:

$$\begin{array}{ccc} Y \times_Y A & \xrightarrow{i'} & Y \\ \downarrow{\scriptstyle \sigma'} & & \downarrow{\scriptstyle \sigma} \\ A & \xrightarrow{i} & Y \end{array}$$

$Y \times_Y A$ è un sottogetto non banale di A in quanto $b \in F(Y \times_Y A)$ e σ' è mono in quanto pullback di mono. Di conseguenza per la connessione di A σ' è un automorfismo di A tale che $F(\sigma')(a) = b$ e l'azione di Aut(A) su F(A) è transitiva. □

Lemma 2.3.3. *Sia A connesso Allora ogni freccia f verso A è epi e quindi F(f) è suriettiva*

Dimostrazione. Possiamo fattorizzare f come un epi seguito da un mono: $f = m \circ e$. Ma A è connesso e quindi m deve essere un isomorfismo e in particolare epi. Quindi f è epi in quanto composizione di epi. □

Proposizione 2.3.4. *J=$\{(A, a) \in I \mid A$ è di Galois$\}$ è cofinale in I.*

Dimostrazione. Dato un $(A, a) \in J$ esiste $(B, b) \in J$ tale $\varphi^B_{(A,a)} : Hom(B, A) \to F(A)$ è biettiva. Una qualunque $f : B \to A$ è tale che $F(f)$ è suriettiva. Quindi $\exists b' \in F(B)$ tale che $Ff(b') = a$ e la tesi si ottiene scegliendo (B, b'). □

Ragionando come nella sezione precedente possiamo definire un funtore $Colim_J$: $C \to Sets$. Dalla proposizione precedente otteniamo subito il seguente corollario.

Corollario 2.3.5. $F \simeq colim_J$

Proposizione 2.3.6. *Se $(A, a), (B, b) \in J$ e $(A, a) \leq (B, b)$ allora $Aut(B)$ agisce transitivamente su $Hom(B, A)$ e si ha $A \simeq \frac{B}{G}$, per qualche $G < Aut(B)$*

Dimostrazione. Possiamo definire un'azione di $Aut(B)$ su $Hom(A, B)$ con $g \cdot \sigma = g \circ \sigma$. Per dimostrare la transitività dell'azione mostriamo che $\forall g \in Hom(B, A)$ $\exists \sigma \in Aut(A)$ tale che $f^B_A \circ \sigma = g$. Sia $g \in Hom(B, A)$ e sia $a' = F(g)(b)$. Poiché f^B_A è suriettiva esiste $b' \in F(B)$ tale che $F(f^B_A)(b') = a'$ e poiché B è di Galois esiste $\sigma \in Aut(B)$ tale $F(\sigma)(b) = b'$. Quindi $F(f^B_A \circ \sigma)(b) = F(f^B_A)(b') = a' = F(g)(b)$ e dall'iniettività di $F^A_{(B,b)}$ segue che $f^B_A \circ \sigma = g$. Sia G lo stabilizzatore dell'azione. Allora $f^B_A = g \circ p$ dove $p : B \to \frac{B}{G}$ e $g : \frac{B}{G} \to A$ sono le mappe canoniche del quoziente. Vogliamo mostrare che g è un isomorfismo. Per farlo notiamo che F(g) è suriettiva, in quanto $F(f^B_A)$ lo è. Inoltre $|F(\frac{A}{G})| = |\frac{F(A)}{G}| = |\frac{Aut(A)}{G}| = |Hom(A, B)| \leq |F(B)|$, dove la prima uguaglianza è dovuta al fatto che F commuta con il passaggio al quoziente, la seconda al fatto che A è di Galois, la terza dal

fatto che l'azione di Aut(A) su Hom(A,B) è transitiva e la disuguaglianza dal fatto che B è connesso. Quindi F(g) è una biezione e per l'assioma 8 segue che g è un isomorfismo. □

Teorema 2.3.7. *Se $(A,a),(B,b) \in J$ e $(A,a) \leq (B,b)$ allora esiste un morfismo di gruppi $\gamma^{(B,b)}_{(A,a)} : Aut(B) \to Aut(A)$ suriettivo. Esplicitamente, dato $\sigma \in Aut(B)$, $\gamma^{(B,b)}_{(A,a)}(\sigma)$ è definito come l'unico automorfismo di A che rende commutativo il seguente diagramma:*

$$\begin{array}{ccc} B & \xrightarrow{f^B_A} & A \\ \downarrow{\scriptstyle \sigma} & & \vdots{\scriptstyle \gamma^{(B,b)}_{(A,a)}(\sigma)} \\ B & \xrightarrow{f^B_A} & A \end{array}$$

Dimostrazione. Poiché A e B sono di Galois, ragionando come nel teorema precedente si trova che $\forall \sigma \in Aut(B)$ esiste un'unica $\alpha \in Aut(A)$ tale che $F(\alpha)(b) = F(f^B_A \circ \sigma)$. Allora possiamo definire $\gamma^{(B,b)}_{(A,a)} : Aut(B) \to Aut(A)$ $\gamma^{(B,b)}_{(A,a)}(\sigma) \mapsto \tau$. La suriettività della mappa si prova ancora ragionando come nel teorema precedente e ricordando che f^B_A è suriettiva Il fatto che sia un omomorfismo di gruppi si mostra notando che $F(\gamma^{(B,b)}_{(A,a)}(\sigma \circ \sigma'))(a) = F(\gamma^{(B,b)}_{(A,a)}(\sigma) \circ \gamma^{(B,b)}_{(A,a)}(\sigma'))(a) =$ e ricordando che l'azione di Aut(A) su F(A) è libera. □

Definizione 2.6. Definiamo π il gruppo profinito limite inverso degli Aut(A) al variare di $(A,a) \in J$.

Osservazione 13. Se $A \in J$ e $a,b \in F(A)$, esiste un unico automorfismo σ di A tale che $\sigma(a) = b$. Di conseguenza $(A,a) \simeq (A,b)$ e la mappa indotta da σ tra Aut(A) e Aut(A) è un isomorfismo. Di conseguenza, possiamo pensare π (rispettivamente F) come limite (rispettivamente colimite) indicizzato tra gli oggetti di Galois invece che dalle coppie $(A,a) \in J$.

2.4 Un'equivalenza di categorie

Definizione 2.7. Definiamo $\pi - sets$ la categoria degli insiemi finiti con un'azione continua di π.

Lemma 2.4.1. *$\forall X \in Ob(C)$ il gruppo profinito π agisce su $F(X) \simeq Colim_J(X)$ e se $h : X \to Y$ allora F(h) è un morfismo di azioni.*

Dimostrazione. Possiamo definire $\gamma : \pi \times F(X) \to F(X)$ $\gamma : ([f],(\sigma_j)_{j\in J}) = [f \circ \sigma_A]$ se $f \in Hom_C(A,X)$. L'applicazione è ben definita in quanto se [f]=[g] con $g \in Hom_C(B,X)$ allora $f = g \circ \psi$ per qualche $\psi \in Hom_C(A,B)$. Ma allora $[f \circ \sigma_A] = [g \circ \psi \circ \sigma_A] = [g \circ \sigma_B \circ \psi] = [g \circ \sigma_B]$. Infine F(h) è

un morfismo di azioni in quanto $F(X) \simeq lim_J(Hom_C(,X))$ naturalmente, e quindi F(h) non è altro che la composizione a sinistra con h. □

Definizione 2.8. Definiamo un funtore $H : C \to \pi - sets$ H(X)=F(X), H(f)=F(f), considerando ogni F(X) dotato dell'azione definita nel teorema precedente.

Osservazione 14. Dimostreremo a breve che il funtore è ben definito, ovvero che l'azione è continua.

Lemma 2.4.2. *Se $A \in Ob(C)$ è connesso allora H(A) è connesso, l'azione di π su H(A) è transitiva e $\forall G \leq Aut(A)$ $H(\frac{A}{G}) \simeq \frac{Aut(A)}{G}$.*

Dimostrazione. Se A è connesso esiste B di Galois e $G \leq Aut(B)$ tale che $A \simeq \frac{B}{G}$. Possiamo definire un'azione continua transitiva di π su Aut(B) tramite moltiplicazione a sinistra. Inoltre poiché B è di Galois $\forall b \in F(B)$ l'applicazione $\psi : Aut(B) \to B$ $\sigma \mapsto F\sigma(b)$ è isomorfismo di $\pi - sets$. Questo isomorfismo passa al quoziente, inducendo una mappa $\gamma : \frac{Aut(B)}{G} \to \frac{F(B)}{G}$ $[f] \mapsto [Ff(a)]$. Questa mappa è suriettiva e poiché i due insiemi sono della stessa cardinalità è una biezione. Quindi $H(\frac{B}{G}) \simeq \frac{Aut(B)}{G}$ come $\pi - sets$. La tesi segue dal fatto che l'azione di π su $\frac{Aut(B)}{G}$ è transitiva in quanto π_B è suriettiva. □

Lemma 2.4.3. *$\forall X \in Ob(C)$ l'azione di π su $F(X)$ è continua.*

Dimostrazione. Notiamo innanzitutto che possiamo ridurci al caso in cui X è connesso, in quanto $\pi^{-1}(x)$ se $x \in F(X)$ dipende solo dalla componente connessa di $x \in F(X)$. Se X è connesso l'azione di π è transitiva e quindi ci è sufficiente dimostrare che Stab(x) è aperto $\forall x \in F(X)$. Ma $F(X) \simeq Hom(A, X)$ per qualche $A \in J$ con l'azione di moltiplicazione sulla A-esima componente. Se $f \in Hom(A, X)$ abbiamo che $Stab(f) = \{(\sigma_j)_{j\in J} | f \circ \sigma_A = f\}$ e che $Ker\pi_A = \pi_A^{-1}(Id_A) \subseteq Stab(f)$ è aperto dove $\pi_A : \pi \to Aut(A)$ è la proiezione canonica. Prendiamo quindi un $\sigma \in Stab(f)$ e costruiamo un suo intorno aperto interamente contenuto in $Stab(f)$. Notiamo che $\sigma \in \sigma_A(Ker\pi_A)$, che è aperto in quanto la moltiplicazione per σ_A sulla A-esima componente è un omeomorfismo. Ci basta quindi mostrare che $\sigma_A(Ker\pi_A) \subseteq Stab(f)$. Se $\gamma \in \sigma_A(Ker\pi_A)$ allora $\gamma * f = f \circ \gamma_A = f \circ \sigma_A = f$ e quindi $\gamma \in Stab(f)$. □

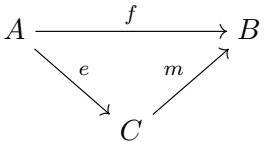
Teorema 2.4.4. *H è un'equivalenza di categorie.*

Dimostrazione. 1. **H è essenzialmente suriettivo** Poiché H è definito come F commuta con i limiti quindi se $A \in Ob(\pi - sets)$, $A \simeq \coprod_{i\in I} A_i$ con A_i connessi e se $A_i \simeq H(Y_i)$ per ogni i e per qualche $Y_i \in Ob(C)$ allora $H(\coprod_{i\in I} Y_i) \simeq \coprod_{i\in I} H(Y_i) \simeq \coprod_{i\in I} A_i \simeq A$. Quindi possiamo limitarci a dimostrare che è essenzialmente suriettivo sui connessi. Sia

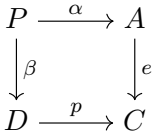
quindi A connesso, allora $A \simeq \frac{Aut(B)}{G} \simeq H(\frac{B}{G})$ per qualche$B \in J$ e qualche $G \leq Aut(B)$

2. **H è fedele** E' sufficiente mostrare che F è fedele. Se $f, g : A \to B$ sono tali che F(f)=F(g) allora il loro equalizzatore $e : E \to A$ è tale che F(e) è iso. Ma F riflette gli isomorfismi, quindi e è un iso e $f \circ e = g \circ e$ implica f=g.

3. **H è pieno** Sia $f : H(A) \to H(B)$. Se $A \simeq \coprod_{i \in I} A_i$ allora dalla proprietà universale del coprodotti segue che
$Hom_C(A, B) \simeq \coprod_{i \in I} Hom_C(A_i, B)$ e poiché H commuta con i coprodotti $Hom_{\pi-sets}(H(A), H(B) \simeq \coprod_{i \in I} Hom_{\pi-sets}(H(A_i), H(B))$.
Possiamo quindi supporre A connesso. Inoltre possiamo fattorizzare f come $m \circ e$ con m mono ed e epi:



Se $p : D \to C$ è un sottoggetto allora possiamo considerare il pullback di e ed p :



Poiché i mono sono stabili per pullback si ha che α è un sottoggetto di X e dalla sua connessione segue che o P è l'oggetto iniziale o α è un isomorfismo. Se P è l'oggetto iniziale allora F(P) è l'insieme vuoto. Poiché F commuta con il pullback e in Set il pullback di un epimorfismo è un epimorfismo, otteniamo un' applicazione suriettiva tra l'insieme vuoto e F(D). Ma allora F(D) è l'insieme vuoto e quindi D è l'oggetto iniziale. Se α è un isomorfismo in particolare è epi e quindi, poiché $p \circ \beta = e \circ \alpha$, p è epi. Ma allora p è mono ed epi e quindi un iso. Quindi C è una componente connessa di B. Di conseguenza se $B \simeq \coprod_{i \in I} B_i$ l'applicazione $\psi : Hom_C(A, B) \to \coprod Hom_C(A, B_i)$ $\psi(f) = e$, dove e è la prima componente della decomposizione epi-mono, è una biezione. Poiché H manda oggetti connessi in oggetti connessi allora la stessa decomposizione vale per $Hom_{\pi-sets}(H(A), H(B))$. Di conseguenza possiamo supporre anche B connesso. Possiamo trovare un X di Galois tale che $A \simeq \frac{X}{G_1}$ e $B \simeq \frac{X}{G_2}$ con G_1 e G_2 sottogruppi di $Aut(X)$ e quindi $H(A) \simeq \frac{Aut(X)}{G_1}$

e $H(B) \simeq \frac{Aut(X)}{G_2}$. Poiché F è fedele e i due insiemi sono finiti di basta dimostrare che $|Hom_C(\frac{X}{G_1}, \frac{X}{G_2})| = |Hom_{\pi-sets}(\frac{Aut(X)}{G_1}, \frac{Aut(X)}{G_2})|$. Innanzitutto notiamo che ogni $f \in Hom_C(\frac{X}{G_1}, \frac{X}{G_2})$ si solleva ad un automorfismo σ di X:

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \frac{X}{G_1} & \xrightarrow{f} & \frac{X}{G_2} \end{array}$$

Infatti poiché X è di Galois e le proiezioni π_i in Set sono suriettive, possiamo scegliere $a, a' \in F(A)$ tali che le $F(\pi_2)(a') = F(f \circ \pi_1)(a)$, un automorfismo σ di X tale che $F(\sigma)(a) = a'$ e la tesi segue allora dalla connessione di X. Ora per la proprietà universale del quoziente $\frac{X}{G_2}$ un automorfismo σdi X dà luogo ad un un morfismo $f \in Hom_C(\frac{X}{G_1}, \frac{X}{G_2})$ se e solo se $\forall g \in G_1 \ \pi_2 \circ \sigma \circ g = \pi_2 \circ \sigma$ e questo avviene se e solo se $\sigma G_1 \subseteq G_2\sigma$. Infatti se $\pi_2 \circ \sigma \circ g = \pi_2 \circ \sigma \ \forall g \in G_1$ allora $\forall g' \in G_2$ $\pi_2 \circ \sigma \circ g = \pi_2 \circ g'\sigma$ e dall'unicità della fattorizzazione $\sigma \circ g = g' \circ \sigma$. Se $\sigma G_1 \subseteq G_2\sigma$ allora $\sigma \circ g = g' \circ \sigma$ e quindi $\pi_2 \circ \sigma \circ g = \pi_2 \circ g' \circ \sigma = \pi_2 \circ \sigma$. Inoltre due automorfismi σ e σ' danno luogo alla stessa f se e solo se $\pi_2 \circ \sigma = \pi_2 \circ \sigma'$ se e solo se $\pi_2 \circ \sigma \circ (\sigma')^{-1} = \pi_2$ se e solo se $\sigma \circ (\sigma')^{-1} \in G_2$ se e solo se $G_2\sigma = G_2\sigma'$. Quindi $|Hom_C(\frac{X}{G_1}, \frac{X}{G_2})| = |\{G_2\sigma | \sigma G_1 \subseteq G_2\sigma\}|$. Con un ragionamento del tutto analogo, ricordando che $Aut(X)$ agisce transitivamente su se stesso per moltiplicazione, si trova che $|Hom_{\pi-sets}(\frac{(Aut(X)}{G_1}, \frac{(Aut(X)}{G_2})| = |\{\sigma G_2 | G_1\sigma \subseteq \sigma G_2\}|$. Poiché i due insiemi sono chiaramente in biezione segue la tesi. □

Definizione 2.9. Definiamo $\pi(C, F)$ il gruppo fondamentale della categoria Galoisiana C con funtore fondamentale F

Capitolo 3

Due esempi: rivestimenti ed estensioni di campi

In quest'ultimo capitolo mostreremo in che senso il gruppo fondamentale di una categoria Galoisiana sia una generalizzazione del gruppo fondamentale di uno spazio topologico e del gruppo di Galois di un'estensione di campi. Definiremo a partire da uno spazio topologico connesso la categoria dei rivestimenti, mostreremo che è una categoria Galoisiana e infine studieremo, sotto alcune ipotesi aggiuntive, il rapporto tra il gruppo fondamentale topologico e il gruppo fondamentale della categoria. Per quanto riguarda le estensioni di campi, costruiremo un'opportuna categoria (la categoria delle estensioni campi non è molto interessante a livello categoriale) che dimostreremo essere Galoisiana e mostreremo come il gruppo fondamentale della categoria Galoisiana coincida, a meno di isomorfismo, con il gruppo di Galois assoluto del campo di partenza.

3.1 Rivestimenti

Definizione 3.1. Un rivestimento di uno spazio topologico X è uno spazio topologico Y con una mappa $p : Y \to X$ suriettiva tale che $\forall x \in X$ esiste un intorno aperto U di x, detto banalizzante, e un omeomorfismo $\alpha : p^{-1}(U) \to U \times p^{-1}(x)$ che rende commutativo il seguente diagramma:

$$\begin{array}{ccc} p^{-1}(U) & \xrightarrow{\alpha} & U \times p^{-1}(x) \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle \pi_1} & \\ & U & \end{array}$$

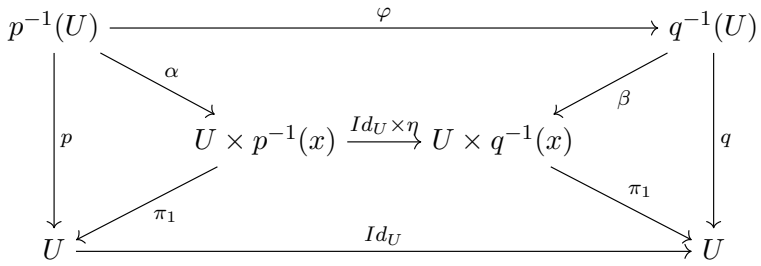
Y si dice rivestimento finito se $p^{-1}(x)$ è finito $\forall x \in X$.

Definizione 3.2. Se (Y,p) e (Z,q) sono rivestimenti di uno spazio topologico X, un morfismo di rivestimenti è un'applicazione continua $\varphi : Y \to Z$ tale che $p = q \circ \varphi$

Osservazione 15. Se φ è un morfismo di rivestimenti allora $\forall x \in X$ φ induce tramite restrizione un'applicazione tra $p^{-1}(x)$ e $q^{-1}(x)$, in quanto se $y \in p^{-1}(x)$ allora $q \circ \varphi(y) = p(y) = x$ e quindi $\varphi(y) \in q^{-1}(x)$.

Definizione 3.3. Indichiamo con Riv_X la categoria dei rivestimenti finiti di X, i cui oggetti sono i rivestimenti di X e i cui morfismi sono i morfismi di rivestimenti.

Lemma 3.1.1 (Lemma fondamentale)**.** *Se (Y,p) e (Z,q) sono rivestimenti di* X $\forall x \in X$ *e* $\varphi : Y \to X$ *è un morfismo di rivestimenti,* $\forall x \in X$ *esistono un intorno aperto* U *di* x *e un'applicazione* $\eta : p^{-1}(x) \to q^{-1}(x)$ *tale che il seguente diagramma commuti:*



Dimostrazione. Per ipotesi esistono due intorni V',V" di x che banalizzano i due rivestimenti. $V = V' \cap V''$ rende commutativi i due triangoli a lato, in quanto essi sono semplicemente la restrizione dei triangoli commutativi degli aperti banalizzanti. V rende anche commutativo il rettangolo esterno in quanto $Id_U \circ p = p = q \circ \varphi$.
Definendo $\psi = \beta \circ \varphi \circ \alpha^{-1}$ abbiamo che $\pi_1 \circ \psi = \pi_1 \circ \beta \circ \varphi \circ \alpha^{-1} = \pi_1$ e quindi $\psi(u, d) = (u, \eta(u, d))$ con $\eta : U \times p^{-1}(x) \to q^{-1}(x)$. Per ottenere la tesi vogliamo mostrare che esiste un intorno U di x tale che $\eta(u, d) = \eta(x, d)$ per ogni $u \in U$ e quindi $\psi = Id_U \times \eta$ in $U \times p^{-1}(x)$. Definiamo $\gamma : V \times p^{-1}(x) \to q^{-1}(x) \times q^{-1}(x)$: $\gamma(u, d) = (\eta(x, d), \eta(u, d))$ che è continua in quanto è continua sulle singole componenti. Chiaramente $\gamma(x, d) \in \Delta$ dove Δ è la diagonale di $q^{-1}(x) \times q^{-1}(x)$ che è un aperto per la topologia prodotto, in quanto questa è la topologia discreta. Per la continuità di γ e la compattezza di $p^{-1}(x)$, ragionando come nel teorema di Wallace, possiamo trovare un intorno aperto nella forma $U \times p^{-1}(x)$ di $\{x\} \times p^{-1}(x)$ tale che $\gamma(U \times p^{-1}(x)) \subset \Delta$. In particolare si ha che $\eta(x, d) = \eta(u, d)$ per ogni $u \in U$ e ogni $d \in p^{-1}(x)$ e quindi possiamo definire $\eta(d) = \eta(x, d)$. □

Lemma 3.1.2. *Sia i rivestimenti finiti che i morfismi di rivestimenti finiti sono applicazioni aperte.*

Dimostrazione. Sia (Y,p) un rivestimento, A un suo aperto e $x = p(y) \in p(A)$. Esiste un intorno aperto U di x tale che $f^{-1}(U)$ è omeomorfo tramite α a $U \times p^{-1}(x)$. $\alpha(y)$ è contenuto, poiché $p^{-1}(x)$ è finito e $\alpha(A)$ è aperto, in un intorno aperto V di $U \times \{d\}$, dove d=$\pi_2 \circ \alpha(y)$. Quindi $\pi_1(V)$ è intorno aperto di x contenuto in $p(A) = \pi_1 \circ \alpha(A)$

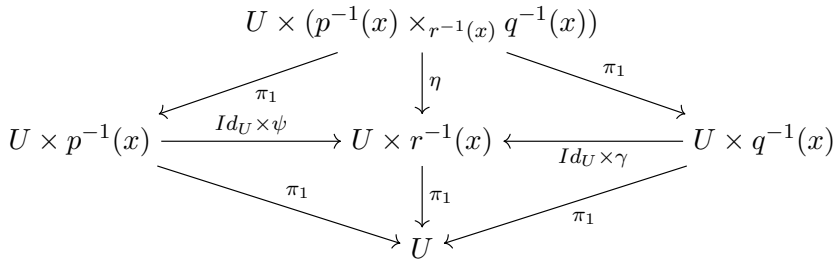
Sia $f : (Y, p) \to (Z, q)$ un morfismo di rivestimenti, A un suo aperto e $z = f(y) \in f(A)$. Allora $q(z) = q \circ f(y) = p(y)$ e scegliamo applicando il lemma fondamentale troviamo un intorno aperto U di p(y) che banalizza entrambi i rivestimenti. Prendendo $V = U \cap p(A)$, che è aperto per la prima parte del teorema, si ha che $q^{-1}(V) = q^{-1}(U \cap p(A)) = q^{-1}(U) \cap q^{-1}(p(A)) \subset q^{-1}(U) \cap f(A)) \subset f(A)$ e quindi $q^{-1}(V)$ è un aperto contenente z dentro f(A). □

Definizione 3.4. Sia X uno spazio topologico e $x \in X$. Se (Y,p) è un rivestimento finito definiamo $F_x(Y, p) = p^{-1}(x)$. Se $f : (Y, p) \to (Z, q)$ è un morfismo di rivestimenti definiamo $F_x(f)$ come la mappa indotta sulla fibra costruita nel lemma fondamentale. Otteniamo in questo modo un funtore $F : Riv_X \to Sets$.

Teorema 3.1.3. *Se X è connesso e $x \in X$ allora (Riv_X, F_x) è una categoria Galoisiana*

Dimostrazione. 1. Riv_X **è finitamente completa**

Il rivestimento banale $Id_X : X \to X$ è l'oggetto terminale. Dobbiamo mostrare che dati tre rivestimenti (Y,p),(Z,q),(W,r) e due morfismi di rivestimenti $\varphi_Y : Y \to W$ e $\varphi_Z : Z \to W$ esiste il loro pullback. Ricordiamo che in Set il pullback è l'insieme $Y \times_W Z$= {(y,z) in $Y \times Z$ tali che $\varphi_Y(y) = \varphi_Z(z)$} e che quindi ci basta mostrare che questo insieme ha una struttura di rivestimento finito. Mostriamo quindi che $p \circ \pi_Y = q \circ \pi_Z : Y \times_W Z \to X$ è un rivestimento. Applicando due volte il lemma precedente troviamo un intorno U di x che banalizza tutti e tre i rivestimenti e quindi possiamo trovare il seguente diagramma commutativo:



$U \times_{r^{-1}(x)} q^{-1}(x))$ è un sottospazio aperto di $U \times r^{-1}(x)$ e η è l'inclusione. Ora, chiamando β l'omeomorfismo tra $U \times r^{-1}(x)$ e $r^{-1}(U)$,$\beta \circ \varphi_Y \circ \pi_Y$ dà una mappa aperta e biettiva e quindi un omeomorfismo tra ($p \circ$

$\pi_Y)^{-1}(U)$ e $U \times (p^{-1}(x) \times_{r^{-1}(x)} q^{-1}(x))$ che fa commutare il seguente diagramma.

$$\begin{array}{ccc} (p \circ \pi_Y)^{-1}(U) & \xrightarrow{\beta \circ \varphi_Y \circ \pi_Y} & U \times (p^{-1}(x) \times_{r^{-1}(x)} q^{-1}(x)) \\ & {\scriptstyle p} \searrow \quad \swarrow {\scriptstyle \pi_1} & \\ & U & \end{array}$$

□

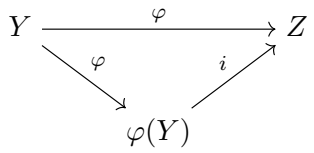
2. **In Riv_X ci sono i coprodotti e un oggetto iniziale**
   Infatti l'unione disgiunta di(Y,p) e (Z,q),$(Y \coprod Z, p \coprod q)$ è il coprodotto con fibra $p^{-1}(x) \coprod q^{-1}(x)$. L'insieme vuoto è invece l'oggetto iniziale.

3. **In Riv_X i quozienti per sottogruppi finiti di automorfismi.**
   Sia G un sottogruppo finito degli automorfismi di un rivestimento (Y,p). Come nel teorema precedente vogliamo mostrare che il quoziente in Set rispetto a G, con la topologia quoziente, è ancora un rivestimento di X, con la mappa continua f indotta in Top. Poiché G è finito e ogni $g \in G$ è un morfismo di rivestimenti possiamo applicare un numero finito di volte il lemma e ottenere $\forall x \in X$ un intorno U di x che banalizza tutti gli elementi di g, cioè troviamo una famiglia di applicazioni ψ_g biettive, che non sono altro che la restrizione alla fibra degli automorfismi, che rendono commutativo il seguente diagramma per ogni $g \in G$

$$\begin{array}{ccc} p^{-1}(U) & \xrightarrow{g} & p^{-1}(U) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ U \times p^{-1}(x) & \xrightarrow{Id_U \times \psi_g} & U \times p^{-1}(x) \end{array}$$

   Di conseguenza possiamo considerare il quoziente di $p^{-1}(x)/G = f^{-1}(x)$ dove stiamo identificando g con ψ_g Una qualsiasi mappa come nel diagramma precedente da $p^{-1}(U)$ a $U \times p^{-1}(x)$ composta con la proiezione al quoziente $U \times p^{-1}(x) \to U \times (p^{-1}(x)/G)$ induce per passaggio al quoziente l'omeomorfismo cercato tra $f^{-1}(U)$ e $U \times p^{-1}(x)/G = U \times f^{-1}(x)$.

4. $\forall\ \varphi : (Y,p) \to (Z,q)$ **ammette una decomposizione epi mono.**
   Notiamo innanzitutto che la restrizione di q a $\varphi(Y)$ è un rivestimento, in quanto per ogni x possiamo scegliere un U come nel lemma fondamentale e $q^{-1}_{|\varphi(Y)}(U) \simeq U \times q^{-1}_{|\varphi(Y)}(x)$. Quindi c'è la seguente fattorizzazione:



dove i è l'inclusione. Poiché i è iniettiva e φ è suriettiva sull'immagine si ha la tesi.

5. **se** $m : (Y, p) \to (Z, q)$ **è mono allora** $\exists T$ **tale che** $Z = Y \coprod T$
   Mostriamo prima che una mappa è epi se e solo è suriettiva e mono se e solo è iniettiva. I se sono ovvi. Se una mappa f : $(Y, p) \to (Z, q)$ non è suriettiva ragionando come nel punto precedente si ottiene che la restrizione di q al complementare di f(Y) è un rivestimento. Possiamo quindi considerare due morfismi:$g \coprod g$ e $g_{f(Y)} \coprod g_{Z \setminus F(Y)}$:$Z \to X \coprod X$. Questi sono due morfismi diversi tali che diventano uguali composti con f. Quindi f non è epi. Se f non è iniettiva allora la mappa $Y \times_Z Y \to Y$ non è biettiva, quindi non può essere un isomorfismo, quindi f non è mono. A questo punto è sufficiente notare che m è aperta e iniettiva, quindi un omeomorfismo con l'immagine e quindi $Z = Y \coprod (Z - m(Y))$

6. $e : (Y, p) \to (Z, p)$ **epi implica** $F_x(e)$ **epi**
   Se e è epi allora la mappa $\psi = F(e)$ del lemma fondamentale è suriettiva, in quanto composizione di funzioni suriettive.

7. F_x **commuta con i limiti, con le somme e con i quozienti**
   E' chiaro dalla costruzione esplicita di limiti somme e quozienti.

8. F_x **riflette gli isomorfismi.**
   Sia $f : (Y, p) \to (Z, q)$ un morfismo di rivestimenti tale che $(F_x(f))$ è biettiva. Mostriamo prima che $(F_a(f))$ $\forall a \in X$ mostrando che l'insieme $A = \{a \in X$ tali che $(F_a(f))$ è biettiva$\}$ è sia aperto che chiuso, la tesi seguirà quindi dalla connessione di X e dal fatto che $x \in A$ Se $a \in A$ per il lemma fondamentale $\exists$ un intorno aperto U di a che banalizza entrambi i rivestimenti. La mappa ψ del lemma è esattamente $(F_a(f))$ che è biettiva. Di conseguenza $f : p^{-1}(U) \to q^{-1}(U)$ è biettiva, in quanto composizione d funzioni biettive e in particolare U è un sottoinsieme aperto di X che contiene a ed è contenuto in A. Quindi A è aperto. Ragionando analogamente si trova che il complementare di A è aperto. Poiché f è aperta ci basta mostrare che è biettiva. Mostriamo che f è suriettiva Infatti se $z \in Z$ per il lemma fondamentale esiste un intorno aperto U di q(z) che banalizza entrambi i rivestimenti. Ma per quanto dimostrato prima $f : p^{-1}(U) \to q^{-1}(U)$ è biettiva e quindi esiste y tale che z=f(y). Mostriamo che f è iniettiva. Infatti se $f(y) = f(y')$ allora $p(y) = q \circ f(y) = q \circ f(y') = p(y')$ e quindi y e

y' appartengono alla stessa fibra. Di conseguenza la tesi segue ancora dal fatto che $(F_{p(y)}(f))$ è biettiva e quindi y=y'

□

Per studiare il rapporto tra il gruppo fondamentale di (X, x) e il gruppo fondamentale della categoria (Riv_X, F_x) supponiamo che X sia localmente connesso per archi e semilocalmente semplicemente connesso. Sotto queste ipotesi si possono classificare tutti i rivestimenti di X, richiamiamo le proposizioni che ci interessano, la cui dimostrazione esula dagli scopi di questo elaborato.

Proposizione 3.1.4. *I rivestimenti finiti connessi di X sono in biezione con i sottogruppi di $\pi_1(X, x)$ di indice finito. La biezione è costruita associando ad ogni rivestimento (Y, p) il sottogruppo $p_*(\pi_1(Y, y))$ dove p_* è la mappa indotta da p sui gruppi fondamentali e $y \in p^{-1}(x)$. In questa biezione l'indice del sottogruppo corrisponde al grado del rivestimento.*

Proposizione 3.1.5. *Nelle notazione del teorema precedente Aut(Y) agisce transitivamente su $p^{-1}(x)$ se e solo se $p_*(\pi_1(Y, y))$ è un sottogruppo normale di $\pi_1(X, x)$. Se questo avviene si dice che il rivestimento è regolare e vale $Aut(Y, y) \simeq \frac{\pi_1(X,x)}{p_*(\pi_1(Y,y))}$ e l'isomorfismo è dato dalla mappa che prende un automorfismo σ e lo manda nella classe dell'unico cammino tale che il punto finale del suo sollevamento con punto iniziale y è $\sigma(y)$.*

Lemma 3.1.6. *Gli oggetti connessi di Riv_X sono i rivestimenti connessi. Gli oggetti di Galois sono i rivestimenti connessi regolari.*

Dimostrazione. Abbiamo mostrato che i monomorfismi sono esattamente i morfismi iniettivi. Poiché i morfismi di rivestimenti sono aperti e chiusi l'immagine di un morfismo iniettivo $(Z, q) \to (Y, p)$ è una componente connessa di Y. Di conseguenza ogni morfismo iniettivo è un isomorfismo se e solo se Y è connesso. La seconda parte del teorema segue direttamente dal teorema precedente. □

Teorema 3.1.7. *Il gruppo fondamentale della categoria Galoisiana (Riv_X, F_x) è isomorfo al completamente profinito di $\pi_1(X, x)$ ovvero al limite inverso dei sottogruppi normali di $\pi_1(X, x)$ ordinati per inclusione, con le mappe di transizione indotte per passaggio al quoziente dalla proiezione canonica.*

Dimostrazione. Per i teoremi precedenti è sufficiente verificare che per ogni $f : (Y, p) \to (Z, q)$, con Y e Z rivestimenti regolari,il seguente diagramma è commutativo:

$$\begin{array}{ccc} \frac{\pi_1(X,x)}{p_*(\pi_1(Y,y))} & \xrightarrow{i} & \frac{\pi_1(X,x)}{q_*(\pi_1(Z,z))} \\ \downarrow{\scriptstyle \alpha_Y} & & \downarrow{\scriptstyle \alpha_Z} \\ Aut(Y) & \xrightarrow{\psi_{YZ}} & Aut(Z) \end{array}$$

dove i è la mappa che manda ogni classe di equivalenza modulo $p_*(\pi_1(Y,y))$ nella stessa classe di equivalenza modulo $q_*(\pi_1(Z,z))$, ben definita perché $p_*(\pi_1(Y,y)) \subseteq q_*(\pi_1(Z,z))$, α_Y, α_Z sono gli isomorfi dati dai teoremi precedenti e ψ_{YZ} è la mappa del sistema inverso costruito nel capitolo due che prende $\sigma \in Aut(Y)$ e lo manda nell'unico $\sigma' \in Aut(Z)$ che fa commutare questo diagramma:

$$\begin{array}{ccc} Y & \xrightarrow{f} & Z \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma'} \\ Y & \xrightarrow{f} & Z \end{array}$$

Poiché l'azione di Aut(Z) su $q^{-1}(x)$ è libera è sufficiente verificare che per ogni $[\beta] \in \frac{\pi_1(X,x)}{p_*(\pi_1(Y,y))}$, $\alpha_z \circ i([\beta])(z) = \psi_{YZ} \circ \alpha_Y([beta])(z)$ per qualche $z \in q^{-1}(x)$. $\sigma = \alpha_Y(\beta)$ è l'unico automorfismo di Y tale che $\sigma(y) = \beta_y(1)$ dove β_y è il sollevamento di β con punto iniziale in y. $\sigma' = \psi_{YZ}(\sigma)$ è l'unico automorfismo di Z tale che $\sigma' \circ f = f \circ \sigma$ cioè tale che $\sigma'(z) = \sigma' \circ f(y) = f \circ \sigma(y) = f(\beta_y(1))$. D'altro canto $i([\beta]) = [\beta]$ e $\alpha_Z(\beta)$ è l'unico automorfismo γ di Z tale che $\gamma(z) = \beta_z(1) = \beta_f(y)(1)$. Ricordando che il sollevamento commuta con le funzioni continue si ha che $\beta_{f(y)}(1) = f(\beta_y(1))$ e quindi $\gamma(1) = \sigma'(1)$. □

3.2 Estensioni di campi

Definizione 3.5. Sia K un campo. Una K-algebra è un anello commutativo unitario $(A, +, \cdot)$ dotato di una struttura di K spazio vettoriale $(A, +, *)$ tale che l'operazione di moltiplicazione dell'anello sia bilineare. Un morfismo di K-algebre è un'applicazione K-lineare che è anche un morfismo di anelli unitari.

Osservazione 16. Ci sono per le K-algebre costruzione analoghe a quelle per gli spazi vettoriali e gli anelli. Infatti si possono definire nello stesso modo il quoziente per un ideale, il prodotto tensoriale di due algebre, dimostrare i teoremi di omomorfismo.

Osservazione 17. Se$(K_i)_{i \in I}$ è una famiglia di estensioni di K allora $\prod_{i \in I} K_i$ ha una naturale struttura di K algebra, con somma e prodotti definiti componente per componente.

Osservazione 18. Se A e B sono estensioni finite separabili di K ogni morfismo $f : A \to B$ di K-algebre è un K-omomorfismo di campi e viceversa.

Definizione 3.6. Una K-algebra è detta separabile se è isomorfa al prodotto finito di estensioni finite e separabili di K.

Definizione 3.7. Sia K un campo e K_s una sua chiusura separabile. Definiamo ${}_KSAlg$ come la categoria che ha come oggetti le K-algebre separabili e come morfismi i morfismi di algebre. Definiamo $F:{}_KSAlg^{op} \to Set$ $F = Hom_{{}_KSAlg}(-, K_s)$

Lemma 3.2.1. *Se A è una K-algebra separabile di dimensione n e K_s è la chiusura separabile di K allora $|Hom_{{}_KSAlg}(A, K_s)| = n$*

Dimostrazione. Sia $A = \prod_{i\in I} A_i$ e indichiamo con e_i l'elemento con tutte le coordinate zero tranne la i-esima. Si ha che $(e_i)^2 = e_i$ e quindi $g(e_i)^2 = g(e_i)$, poiché K_s è un dominio si ha che $g(e_i)$ può essere uguale a zero o a uno. Inoltre $1 = g(1) = g(e_1 + ...e_n) = g(e_1) + ... + g(e_n)$ e quindi $\exists j$ tale che $g(e_j) = 1$. Notiamo che $0 = g(0) = g(e_i)g(e_j)$ per ogni $i \neq j$ e quindi $g(e_i) = 0$. Di conseguenza g è determinato dall'immagine degli elementi di A_j e può essere considerato un omomorfismo di campi tra A_j e K_s. Inoltre ogni omomorfismo di campi t tra A_j e K_s si estende ad un morfismo ψ di K-algebre tra A e K_s, ponendo $\psi(e_j) = t(e_j)$ e $\psi(e_i) = 0$ se $i \neq j$. Quindi $|Hom_{{}_KSAlg}(A, K_s)| = \sum_i |Hom_K((A_i, K_s)|$. Ma poiché ogni A_i è separabile per il teorema dell'elemento primitivo $\exists \alpha_i \in A_i$ tale che $A_i = K[\alpha_i]$. Ma per estensioni di questa forma gli omomorfismi di A_i in K_s sono esattamente tanti quanti il grado del polinomio minimo di α_i cioè la dimensione di A_i su K. Quindi $\sum_i |Hom_K((A_i, \overline{K})| = Dim(A) = n$ □

Lemma 3.2.2. *Per una K-algebra A finitamente generata di dimensione n sono equivalenti:*
1) A è separabile
2) $A \otimes \overline{K} \simeq \overline{K}^n$

Dimostrazione. 1) $\Longrightarrow$ 2) Se A è un'estensione finita e separabile di K, per il teorema dell'elemento primitivo $\exists \alpha$ tale $A = K(\alpha) \simeq \frac{K[X]}{f_\alpha(x)}$ dove $f_\alpha(x)$ è il polinomio minimo di α. Inoltre l'applicazione bilineare $\psi : \overline{K} \times F[X] \to \overline{K}$, $(c, g(x)) \mapsto g(c)$ induce per passaggio al quoziente e per la proprietà universale del prodotto tensoriale un isomorfismo tra $A \otimes \overline{K}$ e $\frac{\overline{K}}{f_\alpha(x)}$. Ora poiché $f_\alpha(x)$ è separabile e si spezza completamente in $\overline{K}$ in fattori distinti di primo grado $x - \alpha_i$, con $0 \leq i < n = Deg(f) \in \mathbb{N}$ distinti fra loro, per il teorema cinese del resto si ha che $\frac{\overline{K}}{f_\alpha(x)} \simeq \frac{\overline{K}}{\prod_1^n x-\alpha_i} \simeq \prod_1^n \frac{\overline{K}}{x-\alpha_i} \simeq \prod_1^n \overline{K}$. Se invece $A = \prod_{i\in I} A_i$ con A_i estensioni finite separabili di K allora $A \otimes \overline{K} = (\prod_{i\in I} A_i) \otimes \overline{K} \simeq \prod_{i\in I}(A_i \otimes \overline{K}) \simeq \overline{K}^n$
2) $\Longrightarrow$ 1) Notiamo innanzitutto che ogni K-algebra B è un dominio se e solo

è un campo, in quanto se è un dominio $\forall b \in B$ l'applicazione $x \mapsto bx$ è un endomorfismo lineare iniettivo, e quindi per questioni dimensionali biettivo. In particolare ogni ideale primo è massimale, in quanto il quoziente per un'ideale è ancora un'algebra finitamente generata e quindi è un dominio se e solo se è un campo. Inoltre l'applicazione canonica $A \to \prod_{m \in M} \frac{A}{m}$ dove M è l'insieme degli ideali massimali è suriettiva, in quanto due ideali massimali sono sempre coprimi, e quindi, sempre per questioni dimensionali, c'è un numero finito di ideali massimali $m_1.....m_i$ per qualche insieme I finito. Il nilradicale $\mathcal{N}$ di A è quindi l'intersezione di ideali massimali, ed essendo A noetheriana è finitamente generato. Quindi esiste N sufficientemente grande tale che $\mathcal{N}^N = (0)$ e in particolare $\prod_{i \in I} m_i^N = (0)$ Quindi per il teorema cinese del resto $A \simeq \prod_{i \in I} \frac{A}{m_i^N}$. Ci rimane da mostrare che $\forall i \in I$ $A_i = \frac{A}{m_i^N}$ è un'estensione separabile di K. Ma ogni A_i è un anello locale, in quanto i suoi ideali massimali corrispondono agli ideali massimali di A che contengono m_i^N e quindi l'unico ideale massimale è $\frac{m_i}{m_i^N}$. Poiché l'unico ideale massimale è anche l'unico ideale primo contiene tutti e soli gli elementi nilpotenti, e tutti gli altri elementi dell'anello sono invertibili. Quindi per mostrare che è un campo ci basta dimostrare che non ci sono elementi nilpotenti non nulli. Per ogni $a \in A$ la sottoalgebra K[a] si immerge iniettivamente in A e tensorizzando questa mappa di immersione con l'applicazione identica di $\overline{K}$ in se stesso troviamo un'applicazione iniettiva di $K[a] \otimes \overline{K}$ in $A \otimes \overline{K} \simeq \overline{K}^n$. Quindi $K[a] \otimes \overline{K}$ non ha idempotenti non nulli. Notiamo che $K[a] \otimes \overline{K} \simeq \frac{K[X]}{f_a} \otimes \overline{K} \simeq \frac{\overline{K}[X]}{(f_a)}$, dove f_a è il polinomio minimo di a su K, tramite l'applicazione di valutazione. Quindi $\frac{\overline{K}[X]}{(f_a)}$ non ha idempotenti non nulli, quindi f_a è separabile. Inoltre se a è nilpotente allora $x^n \in (f_a)$ ma allora $x \in (f_a)$ e quindi a=0. □

Teorema 3.2.3. *${}_K SAlg^{op}$ è una categoria Galoisiana di funtore fondamentale F.*

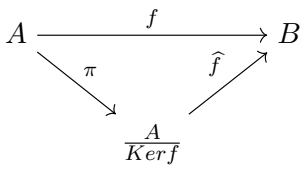
1. ${}_K SAlg$ **ha colimiti finiti**
   Mostriamo che ha coprodotti ed coequalizzatori. Il coequalizzatore di $f, g : A \to B$ è semplicemente il quoziente di B per l'ideale generato dagli elementi nella forma $f(x) - g(x)$. Dobbiamo però mostrare che il quoziente di un'algebra separabile è ancora un'algebra separabile. Se $A = \prod_{i \in I} A_i$ allora una sua sottoalgebra B sarà in particolare un sottomodulo e quindi si scriverà come $\prod_{i \in I} B_i$ con B_i ideali di A_i. Ma gli A_i sono campi e quindi o $B_i = (0)$ o $B_i = A_i$. Quindi $B = \prod_{j \in J} A_i$ per un qualche sottoinsieme J di I. In particolare $\frac{A}{B} \simeq \prod_{i \in I - J} A_i$ Se A e B sono K-algebre il loro prodotto tensoriale, con le immersioni $a \mapsto a \otimes 1$ e $b \mapsto 1 \otimes b$ è il coprodotto in nella categoria delle K-algebre. Infatti ogni coppia f,g di morfismi di algebre $A \to C \leftarrow B$ può essere pensata come una applicazione bilineare $A \times B \to C$ e per la proprietà

universale del prodotto tensoriale esiste un'unico morfismo $A \otimes B \to C$ tale che composto con le immersioni dia f,g. Vogliamo mostrare quindi che il prodotto tensoriale di due K-algebre separabili è una ancora una K-algebra separabile. Ma per il lemma precedente sappiamo che $A \otimes B \otimes \overline{K} \simeq A \otimes \overline{K}^n \simeq \overline{K}^m$ e sempre il lemma precedente ci dà la tesi.

2. ${}_K SAlg$ **ha prodotti e oggetto finale**
   Il campo composto da un solo elemento è chiaramente oggetto finale e il prodotto come K-algebre di due algebre separabili è chiaramente un'algebra separabile.

3. ${}_K Salg^{op}$ **ha i quozienti per un sottogruppo finito degli automorfismi.**
   Sia $A = \prod_{i \in I} A_i$ e G un sottogruppo finito di Aut(A). Vogliamo dimostrare che esiste un oggetto $\frac{A}{G}$ e $i : \frac{A}{G} \to A$ tali che $i \circ g = i \ \forall g \in G$, $\forall f : B \to A$ tale che $g \circ f = f \ \forall g \in G$ esiste un'unica $\psi : B \to \frac{A}{G}$ tale che $i \circ \psi = f$. Consideriamo la sottoalgebra $A^G = \{b \in A \mid g(b) = b \ \forall g \in G\}$ con la mappa di inclusione. Innanzitutto notiamo che la composizione dell'inclusione con un qualsiasi automorfismo in G è ancora l'inclusione, perché ogni automorfismo in G fissa A^G. Inoltre data $f : B \to A$ tale che $g \circ f = f \ \forall g \in G$ si ha che $f(B) \subset B$ e quindi possiamo definire in modo unico $\psi : B \to A^G$ come restrizione di f. Dobbiamo solo mostrare che una sottoalgebra di un'algebra separabile è separabile. Ma se tensorizziamo la mappa di inclusione con $\overline{K}$ possiamo vedere $B \otimes \overline{K}$ come una sottoalgebra di $A \otimes \overline{K} \simeq \overline{K}^n$. Ci siamo quindi ridotti a dimostrare che se K è un campo algebricamente chiuso una sottoalgebra A di K^n è isomorfa a K^m per qualche $m \in \mathbb{N}$. A non ha elementi nilpotenti, di conseguenza il nilradicale $\mathcal{N}$ è nullo. Inoltre ragionando come nei lemmi precedenti troviamo che ci sono solo un numero finito di ideali primi, $m_1 ... m_m$ che sono anche massimali. Quindi $0 = \mathcal{N} = \cap_{0 \leq i \leq m} m_i$ e di conseguenza, per il teorema cinese del resto $A \simeq \prod_{0 \leq i \leq m} \frac{A}{m_i}$. Ma gli $\frac{A}{m_i}$ sono estensioni finite di K e quindi, poiché K è algebricamente chiuso, $\frac{A}{m_i} \simeq K$.

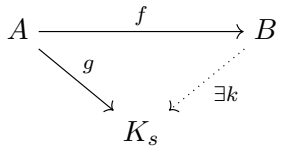
4. **Ogni** $f : A \to B$ **ammette una fattorizzazione mono epi**
   Abbiamo dimostrato nel punto uno che ci sono i quozienti. Quindi possiamo considerare la seguente fattorizzazione:



5. **Se $m : A \to B$ è epi allora esiste C tale che $A = B \coprod C$**

   Se $A = \prod_{i \in I} A_i$ e $m : A \to B$ è epi allora per il punto 1 e il primo teorema di isomorfismo $\exists J \subset I$ tale che $B \simeq \prod_{j \in J} A_j$. Quindi possiamo scegliere $C = \prod_{k \in I - J}$ e ottenere la tesi.

6. **Se $f : A \to B$ è mono allora F(f) è epi**
   Sia $g \in Hom_{_{K}Salg}(A, K_s)$. Vogliamo mostrare che $\exists k \in Hom_{_{K}Salg}(B, K_s)$ che rende commutativo il seguente diagramma.



   Abbiamo dimostrato nel lemma precedente che g è univocamente determinata da l'immagine di una componente diciamo A_j, e viceversa per definire k è sufficiente dire come si comporta su una componente. Poiché f iniettiva $f(\{1\} \times \{1\} ... \times A_j \times \{1\} \times \{1\})$ è un dominio ed è quindi contenuto in una componente di $B = \prod_{t \in T} B_t$ diciamo B_k. Ci siamo ridotti quindi a dimostrare che date due estensioni A e B finite e separabili di K con $A \subset B$ ogni morfismo da A a K_s si estende ad un morfismo tra B e K_s. Poiché B è finita e separabile per il teorema dell'elemento primitivo esiste $\alpha \in B$ tale che $B = A(\alpha)$. Quindi i morfismi di che estendono B sono tanti quanti le radici del polinomio minimo di $\alpha \in K_s$. Ma il polinomio minimo di α è separabile, quindi il suo campo di spezzamento è separabile e quindi è contenuto in K_s. Quindi esiste almeno un morfismo che estende f.

7. **F manda colimiti in limiti, prodotti in coprodotti e quozienti in quozienti**
   Che F manda coequalizzatori in equalizzatore è una semplice verifica che dipende dalla proprietà universale del quoziente di un algebra per un ideale. Inoltre si ha $Hom_{_{K}Salg}(A \otimes B, K_s) \simeq Hom_{_{K}Salg}(A, K_s) \times Hom_{_{K}Salg}(B, K_s)$ per la proprietà universale del prodotto tensoriale. Nel punto precedente abbiamo dimostrato che
   $\varphi : \coprod_{i \in I} Hom_{_{K}Salg}(A_i, K_s) \to Hom_{_{K}Salg}(\prod_{i \in I} A_i, K_s)$ $\varphi(f) = f \circ \pi_j$, se $f \in Hom_{_{K}Salg}(A_i, K_s)$ è una biezione. Notiamo in particolare che $Hom_{_{K}Salg}(A, K_s)$ è finito, in quanto $Hom_{_{K}Salg}(A_i, K_s)$ è finito per ogni i e quindi il funtore è ben definito. Rimane da mostrare che $Hom_{_{K}Salg}(\frac{A}{G}, K_s) \simeq \frac{Hom_{_{K}Salg}(A, K_s)}{G}$ se $G < Aut(A)$ è finito. Per farlo consideriamo l'applicazione $\psi : Hom_{_{K}Salg}(A, K_s) \to Hom_{_{K}Salg}(\frac{A}{G}, K_s) f \mapsto f \circ i$, dove i è l'inclusione di $\frac{A}{G}$ in A, e notiamo che per la proprietà universale del quoziente induce la biezione cercata.

8. **F riflette gli isomorfismi.**
   Se $A = \prod_{i \in I} A_i$ e $B = \prod_{i \in I} B_i$ sono algebre separabili e $f : A \to B$ induce un isomorfismo tra $Hom_{_K Salg}(B, K_s)$ e $Hom_{_K Salg}(A, K_s)$ per il lemma precedente si ha che $Dim(A) = |Hom_{_K Salg}(A, K_s)| = |Hom_{_K Salg}(B, K_s)| = Dim(B)$.Ci basta quindi dimostrare che è f è iniettiva. Se non lo fosse, esisterebbe $a \neq 0 \in A$ tale che f(a)=0. Sia $a_i \in A_i$ una qualunque componente non nulla di a, sia $g : A_i \to K_s$ un qualunque omomorfismo e $h : A \to K_s$ la sua estensione a omomorfismo di algebre. Dato che la mappa indotta da f è suriettiva esiste $k \in Hom_{_K Salg}(B, K_s)$ tale che $k \circ f = h$. Quindi $0 = k \circ f(a) = h(a) = g(a_i)$ ma allora $a_i = 0$ in quanto g è un morfismo di campi. Assurdo.

Lemma 3.2.4. *Gli oggetti connessi in ${}_K SAlg^{op}$ sono le estensione finite separabili di K. Gli oggetti di Galois sono le estensioni finite di Galois di K.*

Dimostrazione. Gli oggetti connessi in ${}_K SAlg^{op}$ sono gli oggetti A tali che se $e : A \to B$ è epi e B non è banale allora e è un isomorfismo. Se A è campo è un'estensione finita separabile di K. Inoltre poiché ogni mappa che parte da un campo è iniettiva segue la tesi. Se A non è campo allora $A = \prod_{i \in I} A_i$ con I con almeno due elementi. Quindi la proiezione su uno dei due fattori è un epimorfismo che non è un isomorfismo e quindi A non è connesso. Un oggetto A connesso è di Galois se e solo se agisce transitivamente su $Hom_{_K SAlg}(A, K_s)$. Poiché A è un'estensione separabile di K $A = K(\alpha)$ per qualche $\alpha \in A$. Gli omomorfismi di A in K_s sono univocamente determinati dall'immagine di α di conseguenza l'azione di $Aut(A)$ su $Hom_{_K SAlg}(A, K_s)$ è transitiva se e solo se l'azione di Aut(A) su α è transitiva se e solo il polinomio minimo f_α di α spezza in A se e solo se A è il campo di spezzamento di f_α se e solo se A è un'estensione di Galois. □

Teorema 3.2.5. *Il gruppo fondamentale π di ${}_K SAlg^{op}$ è isomorfo a $G = Gal(K_s|K) = Aut_K(K_s)$*

Dimostrazione. Sappiamo che $\pi = lim_J Aut(A)$ dove A varia fra le estensioni finite di Galois di K. Notiamo inoltre che nel caso dei campi, le mappe che realizzano il sistema inverso non sono altro che la restrizione degli automorfismi. Per ogni $A \in J$ possiamo definire un morfismo $G \to A$ tramite restrizione. Poiché le restrizioni commutano fra loro otteniamo un'unica mappa $\psi : G \to \pi$. Esplicitamente $\psi(g) = (g_{|A})_{A \in J}$. Vogliamo mostrare che questa mappa è un isomorfismo. E' iniettiva in quanto se $g \in G$ e $g \neq 1_G$ esiste un $x \in K_s$ tale che g$(x) \neq x$. Ma $x \in A$ per qualche A in J,quindi $g_{|A}(x) \neq x$ e di conseguenza $(g_{|A})_{A \in J} \neq 1_\pi$. E' suriettiva in quanto se $(g_{|A})_{A \in J} \in \pi$ possiamo definire $g(x) = g_{|A}$ quando $x \in A$. L'applicazione è ben definita in quanto se $x \in A \cap B$ con $A, B \in J$ poiché il limite è inverso e le mappe sono le restrizioni allora $g_{|A}$ coincide con $g_{|B}$ sull'intersezione. □

Bibliografia

[1] H. Lenstra, *Galois theory for schemes*. Internet, 2008.

[2] R. Douady e A. Duady, *Algèbre et théories galoisiennes*. Cassini, 2005.

[3] M. Manetti, *Topologia*. Springer, 2008.

[4] J. Milne, *Fields and Galois Theory*. Internet, 2014.

[5] G. Patrizi, *Gruppi Profiniti ed Estensioni di Galois di Grado Infinito*. Internet, tesi di laurea specialistica in matematica 2010.

[6] F. Borceux, *Handbook of Categorical Algebra, volume I*. Encyclopedia of Mathematics and its Applications 50, Cambridge University Press, 1994.

[7] S. Mac Lane, *Categories for the Working Mathematician*. Springer, 1998.

[8] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics, 1994.