UNIVERSITÀ DI PISA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Matematica

Tesi di Laurea triennale

Teoria di Galois su superfici di Riemann: rivestimenti ramificati e algebre étale

Candidato:
Vincenzo Galgano

Relatore:
Prof. **Marco Franciosi**

Anno Accademico 2015/2016

A nonna Nina e nonno Cosimo.

A Salvatore Monaco,
che mi ha insegnato ad amare la Vita.

O Captain! my Captain! our fearful trip is done,
The ship has weather'd every rack, the prize we sought is won,
The port is near, the bells I hear, the people all exulting,
While follow eyes the steady keel, the vessel grim and daring;
- Walt Whitman

Indice

Introduzione **5**

1 Prime Nozioni **9**
1.1 Teoria delle categorie 9
1.2 Gruppi profiniti 13
1.3 Rivestimenti topologici 17

2 Teoria di Galois di Grothendieck **23**
2.1 Estensioni di campi e algebre étale 23
2.2 Teoria di Galois finita 27
2.3 Teoria di Galois infinita 33

3 Superfici di Riemann ed estensioni di campi **39**
3.1 Rivestimenti ramificati su superfici di Riemann 39
3.2 Equivalenza tra rivestimenti ramificati e algebre étale 46
3.3 Estensioni di $\mathbb{C}$ di grado di trascendenza 1 55

4 Su due gruppi di Galois assoluti **59**
4.1 Gruppo di Galois assoluto di $\mathbb{C}(Z)$ 59
4.2 *Dessins d'enfant* 67

Introduzione

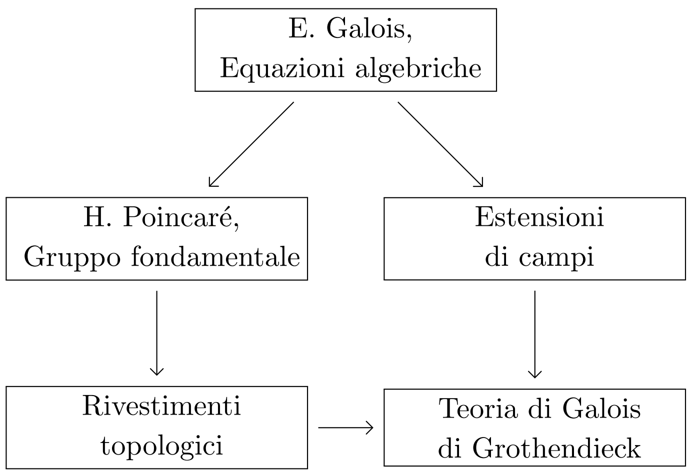
Uno degli strumenti più potenti (e delicati) per studiare diverse strutture algebriche e le relazioni tra esse è senza dubbio il linguaggio della teoria delle categorie, introdotto per la prima volta nel 1945 da S. Eilenberg e S. Mac Lane (nell'ambito della topologia algebrica) e successivamente approfondito dal gruppo di matematici Bourbaki. Tra di essi, il matematico apolide Alexander Grothendieck (1928-2014) è stato il pioniere delle nuove basi della geometria algebrica, introducendo negli anni '50 e '60 il concetto di schema e la teoria dei fasci, generalizzando così il concetto di varietà algebrica.

Tuttavia quando si parla di relazioni tra diverse strutture matematiche non si può non nominare il matematico francese Evariste Galois (1811-1832), a buon diritto considerato uno dei padri dell'algebra astratta: le sue idee sono state i prodromi della teoria dei gruppi. Con la "teoria di Galois" nasce un ponte tra il mondo (o meglio, la categoria) dei gruppi e quello dei campi. Ma più che i suoi risultati, è stata la sua visione poliedrica della matematica a dare importanti contributi nelle varie branche. La sua teoria, che collegava tra loro gruppi e campi, è stata nel XX secolo estesa a diverse strutture, portando i matematici a parlare di teoria di Galois algebrica, topologica e differenziale (cf. [6] e [13]).

Il primo passo verso la generalizzazione della teoria di Galois classica è stato sostituire le estensioni di campi con algebre commutative su un campo finite e separabili (dette étale). Grazie a Grothendieck, la teoria classica è divenuta un caso particolare di una teoria ben più generale, la teoria di Galois di Grothendieck, che si basa su un'equivalenza di categorie tra le categorie $\mathfrak{D}_L$ delle K-algebre finite diagonalizzate da un'estensione di Galois finita L/K e G-$\mathfrak{FSet}$ degli insiemi finiti su cui agisce il gruppo di Galois $G = \mathrm{Gal}(L/K)$ (nel caso finito), e tra le categorie $\mathfrak{A}$ delle K-algebre separabili e $\mathbb{G}$-$\mathfrak{Prof}$ degli spazi profiniti su cui il gruppo di Galois $\mathbb{G} = \mathrm{Gal}(\Omega_s/K)$ della chiusura separabile di K agisce con continuità (nel caso infinito). Il passo successivo è stato quello di estendere tale teoria dalle algebre su un campo ai moduli (su un anello), entrando in una nuova teoria di Galois per anelli introdotta nel 1960 dai matematici M. Auslander e O. Goldman e completata nel 1974 dal matematico A. R. Magid.

In ambito topologico l'eredità di Galois ha avuto come protagonisti i rivestimenti di spazi topologici e i relativi gruppi fondamentali. Tuttavia, anche in questo caso, questo ponte è stato un (altro) caso particolare della teoria degli schemi di Grothendieck e del suo gruppo fondamentale étale (cf. [3]).

Le idee che stanno alla base di queste teorie innovative si possono vedere ben espresse considerando le superfici di Riemann. Il teorema di esistenza di Riemann stabilisce una corrispondenza biunivoca da un lato tra rivestimenti topologici finiti e rivestimenti analitici finiti, dall'altro tra superfici di Riemann compatte e curve algebriche (cf. [5]). In particolare, le analogie tra la teoria di Galois di Grothendieck e la teoria dei rivestimenti si concretizzano in un'(anti)equivalenza di categorie nel caso di superfici di Riemann: tale risultato è l'oggetto centrale di questa trattazione.



Dall'antiequivalenza di categorie tra la categoria $\mathfrak{V}_B$ dei rivestimenti ramificati analitici finiti di una superficie di Riemann connessa e compatta B, e la categoria $\mathfrak{E}_B$ delle algebre étale sul campo $\mathscr{M}(B)$ delle funzioni meromorfe su B, si ha una corrispondenza tra i rivestimenti ramificati analitici finiti connessi regolari e le estensioni di campi di Galois del campo $\mathscr{M}(B)$ (cf. [9]).

Queste relazioni tra oggetti geometrici e oggetti algebrici trovano terreno fertile nell'ambito della geometria algebrica: infatti le categorie equivalenti delle curve algebriche complesse (con morfismi le funzioni regolari) e delle superfici di Riemann compatte (con morfismi le mappe olomorfe) sono a loro volta equivalenti alla categoria delle estensioni di campi di grado di trascendenza 1 su $\mathbb{C}$ (con morfismi gli omomorfismi di $\mathbb{C}$-algebre). Tale equivalenza è riassunta brevemente nella seguente tabella:

Superfici di Riemann compatte e connesse	Campi di funzioni meromorfe
Superfici di Riemann compatte e connesse su $\mathbb{P}^1$	Estensioni di tipo finito di $\mathbb{C}(Z)$
Mappa olomorfa $X \to B$	Estensione di campi $K \subset L$
Mappa meromorfa $X \to \mathbb{P}^1$	Polinomio irriducibile su $\mathbb{C}(Z)$
Grado di una mappa olomorfa $X \to B$	Grado di un'estensione di campi $K \subset L$
Mappa olomorfa $X \to B$ con gruppo di automorfismi G	Estensione di campi $K \subset L$ con gruppo di Galois G

Questa corrispondenza tra superfici di Riemann compatte e connesse ed estensioni di $\mathbb{C}(Z)$ trova un'importante applicazione nel calcolo del gruppo di Galois assoluto di $\mathbb{C}(Z)$, ossia del gruppo di Galois della sua chiusura algebrica. In generale, il gruppo di Galois assoluto di un campo K è il gruppo di Galois della chiusura separabile di K ed il suo calcolo è un problema interessante poichè fornisce informazioni su tutte le estensioni di Galois di K. In questa trattazione analizziamo i casi in cui $K = \mathbb{C}(Z)$ e $K = \mathbb{Q}$.

Nel primo caso, il gruppo di Galois assoluto è stato completamente esplicitato, rispondendo quindi positivamente al problema inverso di Galois sul campo $\mathbb{C}(Z)$: ogni gruppo finito è il gruppo di Galois di un'estensione di $\mathbb{C}(Z)$. Nel secondo caso, il calcolo del gruppo di Galois assoluto di $\mathbb{Q}$ (e quindi il problema inverso di Galois su $\mathbb{Q}$) è ancora un problema aperto. Tuttavia grazie ai risultati fin ora esposti e ad un'intuizione di Grothendieck, è possibile dedurre informazioni su tale gruppo di Galois assoluto facendolo agire su un insieme di grafi bipartiti, chiamati da Grothendieck stesso *dessins d'enfant*, che si immergono in particolari superfici di Riemann, dette aritmetiche, corrispondenti a curve algebriche su campi di numeri: lo studio algebrico dell'azione del gruppo di Galois assoluto di $\mathbb{Q}$ su tali curve algebriche si riduce ad uno studio combinatoriale delle trasformazioni dei rispettivi grafi.

Vediamo ora quali argomenti saranno affrontati nei vari capitoli di questa trattazione.

Nel capitolo 1 diamo una breve introduzione alla teoria delle categorie e alla teoria dei rivestimenti, concentrandoci su alcuni risultati inerenti i gruppi profiniti.

Nel capitolo 2 estendiamo la teoria di Galois classica alla teoria di Galois di Grothendieck, proponendo quindi un approccio categoriale ad un certo tipo di algebre su un campo, dette étale, che rappresentano una generalizzazione delle estensioni di campi di Galois. In particolare, analizzeremo sia la teoria finita che quella infinita.

Nel capitolo 3 introduciamo le superfici di Riemann e i rivestimenti ramificati per poi dedicarci al risultato centrale della trattazione: l'(anti)equivalenza di categorie tra la categoria dei rivestimenti ramificati analitici finiti di una superficie di Riemann compatta e connessa, e la categoria delle algebre étale sul campo delle funzioni meromorfe su tale superficie. Infine, mostriamo che, grazie a tale antiequivalenza, le superfici di Riemann compatte e connesse corrispondono alle estensioni di tipo finito di grado di trascendenza 1 su $\mathbb{C}$.

Nel capitolo 4 ci concentriamo su due gruppi di Galois assoluti: nel caso del campo $\mathbb{C}(Z)$ sapremo calcolare esplicitamente il suo gruppo di Galois assoluto definendo il gruppo fondamentale di uno spazio topologico rispetto ad un germe di cammini; nel caso del campo $\mathbb{Q}$ daremo solo un breve accenno al teorema di Belyi (1979).

Capitolo 1

Prime Nozioni

In questo capitolo diamo una breve introduzione alla teoria delle categorie, enunciando tutti quei risultati che saranno necessari per raggiungere i nostri scopi. In particolare, presentiamo la categoria $\mathfrak{ProfGr}$ dei gruppi profiniti e la categoria G-$\mathfrak{Prof}$ degli spazi profiniti su cui è definita l'azione di un gruppo G. Infine, esponiamo brevemente le definizioni e i risultati principali della teoria classica dei rivestimenti.

I risultati esposti in questo capitolo fanno espresso riferimento all'esposizione *Algèbre et théorie galoisiennes* di R. & A. Douady [9, Cap II,IV]. Per le dimostrazioni omesse in questo capitolo è possibile consultare la referenza citata.

1.1 Teoria delle categorie

Introduciamo alcune nozioni di base della teoria delle categorie che ci permetteranno di mostrare alcune equivalenze, oggetto di questa tesi.

Definizione. Una *categoria* $\mathscr{C}$ è una collezione di oggetti $Obj(\mathscr{C})$ su cui sono definite delle mappe, dette *morfismi*, associate ad un oggetto sorgente X e ad un oggetto destinazione Y e indicate con $\mathrm{Hom}_{\mathscr{C}}(X, Y)$. Per tali morfismi è definita l'applicazione di composizione da $\mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z)$ a $\mathrm{Hom}(X, Z)$ con $(f, g) \mapsto g \circ f$ che è associativa; per ogni X in $\mathscr{C}$, esiste $\mathbb{1}_X$ in $\mathrm{Hom}(X, X)$ tale che, per ogni Y in $\mathscr{C}$ e per ogni f in $\mathrm{Hom}(X, Y)$, si ha $f \circ \mathbb{1}_X = f$ e, per ogni g in $\mathrm{Hom}(Y, X)$, $\mathbb{1}_Y \circ g = g$.

Sebbene non sia formale usare il linguaggio insiemistico per le categorie, si scrive $X \in Obj(\mathscr{C})$ (ma per comodità scriveremo $X \in \mathscr{C}$) per dire che "X è un oggetto di $\mathscr{C}$" e $f \in \mathrm{Hom}(X, Y)$ per dire che "f è un morfismo da X in Y". Per lo stesso motivo, useremo senza troppi formalismi anche quantificatori, connettivi e ogni altro simbolo (i.e. $\subset$, $\in$).

Definizione. Un morfismo $f \in \mathrm{Hom}(X,Y)$ è detto *isomorfismo* se esiste $g \in \mathrm{Hom}(Y,X)$ tale che $g \circ f = \mathbb{1}_X$ e $f \circ g = \mathbb{1}_Y$.
Date due categorie $\mathscr{C}$ e $\mathscr{C}'$, $\mathscr{C}'$ è detta *sottocategoria* di $\mathscr{C}$ se

- $\mathscr{C}' \subset \mathscr{C}$ (ossia tutti gli oggetti di $\mathscr{C}'$ sono anche oggetti di $\mathscr{C}$);
- $\forall X,Y \in \mathscr{C}'$, $\mathrm{Hom}_{\mathscr{C}'}(X,Y) \subset \mathrm{Hom}_{\mathscr{C}}(X,Y)$;
- la composizione in $\mathscr{C}'$ è indotta da quella in $\mathscr{C}$;
- $\mathbb{1}_{X,\mathscr{C}'} = \mathbb{1}_{X,\mathscr{C}}$.

Una sottocategoria $\mathscr{C}' \subset \mathscr{C}$ è *piena* se $\mathrm{Hom}_{\mathscr{C}'}(X,Y) = \mathrm{Hom}_{\mathscr{C}}(X,Y)$ per ogni $X,Y \in \mathscr{C}'$. Date $\mathscr{C}'$ e $\mathscr{C}''$ categorie, la *categoria prodotto* è la categoria $\mathscr{C} = \mathscr{C}' \times \mathscr{C}''$ con $\mathrm{Hom}_{\mathscr{C}}((X',X''),(Y',Y'')) \cong \mathrm{Hom}_{\mathscr{C}'}(X',Y') \times \mathrm{Hom}_{\mathscr{C}''}(Y',Y'')$ e la composizione che passa alle componenti. Data $\mathscr{C}$ categoria, la *categoria opposta* a $\mathscr{C}$ è la categoria $\mathscr{C}^\circ$ avente gli stessi oggetti di $\mathscr{C}$ e i morfismi tali che $\mathrm{Hom}_{\mathscr{C}^\circ}(X,Y) = \mathrm{Hom}_{\mathscr{C}}(Y,X)$ con $g \circ_{\mathscr{C}^\circ} f = f \circ_{\mathscr{C}} g$.

Definizione. Date $\mathscr{C}$ e $\mathscr{C}'$ categorie, una mappa F da $\mathscr{C}$ in $\mathscr{C}'$ si dice

- *funtore covariante* se per ogni $X,Y \in \mathscr{C}$ vale

$$F_{X,Y} : \mathrm{Hom}_{\mathscr{C}}(X,Y) \to \mathrm{Hom}_{\mathscr{C}'}(F(X),F(Y))$$

$$F_{X,Z}(g \circ f) = F_{Y,Z}(g) \circ F_{X,Y}(f)$$
$$F_{X,X}(\mathbb{1}_X) = \mathbb{1}_{F(X)}$$

- *funtore controvariante* se per ogni $X,Y \in \mathscr{C}$ vale

$$F_{X,Y} : \mathrm{Hom}_{\mathscr{C}}(X,Y) \to \mathrm{Hom}_{\mathscr{C}'}(F(Y),F(X))$$

$$F_{X,Z}(g \circ f) = F_{X,Y}(f) \circ F_{Y,Z}(g)$$
$$F_{X,X}(\mathbb{1}_X) = \mathbb{1}_{F(X)}$$

Se F è controvariante, si indica $f \mapsto f^*$; se F è covariante, si indica $f \mapsto f_*$. Date $\mathscr{C},\mathscr{C}'$ e $\mathscr{C}''$ categorie con i funtori $F : \mathscr{C} \to \mathscr{C}'$ e $G : \mathscr{C}' \to \mathscr{C}''$, il *funtore composto* di F e G è il funtore $G \circ F : \mathscr{C} \to \mathscr{C}''$ tale che $(G \circ F)(\cdot) = G(F(\cdot))$ e, per ogni $X,Y \in \mathscr{C}$ e per ogni $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$, vale $(G \circ F)_{X,Y}(f) = G_{F(X),F(Y)}(F_{X,Y}(f))$.

Notiamo che F è controvariante da $\mathscr{C}$ in $\mathscr{C}'$ se e soltanto se F è covariante da $\mathscr{C}^\circ$ in $\mathscr{C}'$. Inoltre, il composto di due funtori entrambi covarianti (o controvarianti) è covariante, altrimenti è controvariante.

Esempi. Sono categorie $\mathfrak{Set}_U$ (insiemi in U), $\mathfrak{Gr}_U$ (gruppi con omomorfismi di gruppo), $\mathfrak{Rg}_U$ (anelli commutativi con omomorfismi di anello), A-$\mathfrak{mod}_U$ (A-moduli con applicazioni A-lineari), $\mathfrak{Top}_U$ (spazi topologici con applicazioni continue), $\mathfrak{Met}_U \subset \mathfrak{Top}_U$ (sottocategoria piena degli spazi metrizzabili), $\mathfrak{LocRg}_U \subset \mathfrak{Rg}_U$ (la sottocategoria non piena degli anelli locali).
Data $\mathscr{C}$ categoria e $X \in \mathscr{C}$, sono funtori:

- (covariante) $\check{X} : \mathscr{C} \to \mathfrak{Set}$ con $Y \mapsto \mathrm{Hom}(X, Y)$: per ogni $Y, Z \in \mathscr{C}$, $f \in \mathrm{Hom}(Y, Z)$ e $h \in \mathrm{Hom}(X, Y)$ si ha $f_*(h) = f \circ h$;
- (controvariante) $\hat{X} : \mathscr{C} \to \mathfrak{Set}$ con $Y \mapsto \mathrm{Hom}(Y, X)$: per ogni $Y, Z \in \mathscr{C}$, $f \in \mathrm{Hom}(Y, Z)$ e $h \in \mathrm{Hom}(Z, X)$ si ha $f^*(h) = h \circ f$.

Definizione. Sia G un gruppo. Un G-insieme è un insieme su cui è definita un'operazione $(g, x) \mapsto g \cdot x$.

Fissato G, la collezione G-$\mathfrak{Set}$ di tutti i G-insiemi è una categoria i cui morfismi sono G-lineari, ossia dato f un morfismo tra due G-insiemi, vale $f(g \cdot x) = g \cdot f(x)$. Inoltre, definiamo il funtore $\omega_G : G\text{-}\mathfrak{Set} \to \mathfrak{Set}$ (detto d'*oblio*) come il funtore che a ogni G-insieme associa l'insieme stesso senza la G-struttura.

Possiamo parlare anche di categorie di funtori. Siano $\mathscr{C}, \mathscr{C}'$ due categorie: costruiamo una categoria prendendo per oggetti i funtori da $\mathscr{C}$ in $\mathscr{C}'$ e per morfismi i morfismi di funtori. Se $\Phi : F \to G$ e $\Psi : G \to H$ sono morfismi di funtori, definiamo la composizione $\Psi \circ \Phi$ come $(\Psi \circ \Phi)_X = \Psi_X \circ \Phi_X$ per ogni $X \in \mathscr{C}$. Un morfismo di funtori $\Phi : F \to G$ è *isomorfismo di funtori* (e indichiamo $F \sim G$) se esiste un morfismo di funtori $\Psi : G \to F$ tale che $\Psi \circ \Phi = \mathbb{1}_F$ e $\Phi \circ \Psi = \mathbb{1}_G$. Notiamo che $\Phi : F \to G$ è isomorfismo di funtori se e solo se per ogni $X \in \mathscr{C}$ il funtore $\Phi_X : F(X) \to G(X)$ è isomorfismo.

Introduciamo ora il concetto di equivalenza tra categorie, che permette di verificare facilmente risultati altrimenti di difficile dimostrazione.

Definizione. Date $\mathscr{C}$ e $\mathscr{C}'$ categorie e $F, G : \mathscr{C} \to \mathscr{C}'$ funtori, un *morfismo funtoriale* da F a G è una mappa Φ per cui, per ogni $X \in \mathscr{C}$, è definito $\Phi_X : F(X) \to G(X)$ tale che $\forall f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ il diagramma seguente commuta

$$\begin{tikzcd} F(X) \arrow[r, "F(f)"] \arrow[d, "\Phi_X"'] & F(Y) \arrow[d, "\Phi_Y"] \\ G(X) \arrow[r, "G(f)"'] & G(Y) \end{tikzcd}$$

Un funtore $F : \mathscr{C} \to \mathscr{C}'$ è *essenzialmente surgettivo* se $\forall X' \in \mathscr{C}'$ $\exists X \in \mathscr{C}$ tale che X' sia isomorfo a $F(X)$. Un funtore $F : \mathscr{C} \to \mathscr{C}'$ è *fedele* (risp. *pienamente fedele*) se, $\forall X, Y \in \mathscr{C}$, $F_{X,Y} : \mathrm{Hom}_{\mathscr{C}}(X, Y) \to \mathrm{Hom}_{\mathscr{C}'}(F(X), F(Y))$ è iniettiva (risp. bigettiva).

Definizione. Un funtore covariante $F : \mathscr{C} \to \mathscr{C}'$ è un'*equivalenza* di categorie se F è pienamente fedele ed essenzialmente surgettivo, o equivalentemente se esiste $G : \mathscr{C}' \to \mathscr{C}$ funtore (detto *quasi-inverso*) tale che $G \circ F \sim \mathbb{1}_{\mathscr{C}}$ e $F \circ G \sim \mathbb{1}_{\mathscr{C}'}$.
Se F è controvariante, allora F è detto *anti-equivalenza* se è un'equivalenza da $\mathscr{C}^{\circ}$ a $\mathscr{C}'$.

Il problema dell'universo

Fin ora non ci siamo posti il problema di precisare in quale universo lavorare. Mostriamo dunque che effettivamente nel nostro caso il problema non sussiste e che estendendo l'universo in cui lavorare si ottiene una categoria equivalente a quella iniziale: ciò grazie ad un lemma di cardinalità.

Siano $U \subset U'$ insiemi: supponiamo che $\forall X \in U$ $\mathcal{P}(X) \subset U$. Sia $\mathscr{C}$ una categoria avente gli oggetti in U': supponiamo che esista un funtore d'oblio $\Omega : \mathscr{C} \to \mathfrak{Set}_U$ e che, $\forall X \in \mathscr{C}$ e $\forall f : \Omega(X) \to F \in U'$ bigezione, esistano $Y \in \mathscr{C}$ e $\phi : X \to Y$ tale che $\Omega(Y) = F$ e $\Omega(\phi) = f$. Notiamo con $\mathscr{C}_U$ la sottocategoria piena di $\mathscr{C}$ formata dagli oggetti di $\mathscr{C}$ soggiacenti in U. Indichiamo la cardinalità di un insieme E con $\#E$. Vale allora il seguente lemma, per la cui dimostrazione si fa riferimento a [9, § 2.3.7].

Lemma 1.1.1 (Lemma di cardinalità)**.** Se esiste $E \in U$ tale che $\forall X \in \mathscr{C}$ valga $\#\Omega(X) \leq \#E$, allora il morfismo di inclusione $\mathscr{C}_U \hookrightarrow \mathscr{C}$ è un'equivalenza di categorie.

Tale risultato permette di mostrare che la categoria dei rivestimenti di uno spazio topologico e la categoria delle estensioni algebriche di un campo non dipendono dalla scelta dell'universo.

Vediamo ora particolari funtori, detti rappresentabili. Data $\mathscr{C}$ categoria, ricordiamo che per ogni $X \in \mathscr{C}$ è definito il funtore controvariante $\hat{X} : \mathscr{C} \to \mathfrak{Set}$ dato da $\hat{X}(Y) = \mathrm{Hom}(Y, X)$.

Definizione. Sia $\mathscr{C}$ una categoria. Un funtore controvariante $F : \mathscr{C} \to \mathfrak{Set}$ è *rappresentabile* se esiste $X \in \mathscr{C}$ per cui $F \cong \hat{X}$.

Lemma (Yoneda)**.** Siano $\mathscr{C}$ categoria, $F : \mathscr{C} \to \mathfrak{Set}$ controvariante e $X \in \mathscr{C}$. C'è una corrispondenza biunivoca tra i morfismi da $\hat{X}$ in F e gli elementi di $F(X)$, data dalla bigezione

$$\theta \in F(X) \longmapsto (\hat{\theta}_Y)_{Y \in \mathscr{C}}$$

dove (per $Y \in \mathscr{C}$ e $f \in \mathrm{Hom}(Y, X)$) $\hat{\theta}_Y : \hat{X}(Y) \to F(Y)$ è data da $\hat{\theta}_Y(f) = f^*(\theta)$.

Per la dimostrazione del risultato appena visto si fa riferimento a [9, § 2.4.3].

1.2 Gruppi profiniti

Definizione. Un insieme I è *parzialmente ordinato* se è munito di una relazione $\leq$ riflessiva, transitiva e antisimmetrica. Un insieme parzialmente ordinato $(I, \leq)$ è detto *filtrante* se $\forall i, j \in I$ esiste $k \in I$ tale che $i, j \leq k$.

Definizione. Sia $\mathscr{C}$ una categoria e $(I, \leq)$ un insieme filtrante. Un *sistema proiettivo* in $\mathscr{C}$ indicizzato da I è una famiglia $(X_i)_{i \in I}$ di oggetti di $\mathscr{C}$ per cui, $\forall (i, j) \in I^2$ tale che $i \leq j$, sono definiti dei morfismi $f_{ij} : X_j \to X_i$ tali che:

i) $\forall i \in I$, $f_{ii} = id_{X_i}$;

ii) $\forall i, j, k \in I$ con $i \leq j \leq k$, $f_{ij} \circ f_{jk} = f_{ik}$.

Indichiamo tale sistema proiettivo con $((X_i)_i, (f_{ij})_{i \leq j})_I$ o, in assenza di ambiguità, semplicemente (X_i).

Definizione. Dato $(X_i, (f_{ij})_{i \leq j})_I$ un sistema proiettivo, definisco il suo *limite proiettivo* come l'elemento universale della categoria $(X = \varprojlim X_i, (p_i)_I)$ per il sistema, con $p_i : X \to X_i$ tale che fa commutare il diagramma

$$\begin{tikzcd} X_j \arrow[r, "f_{ij}"] & X_i \\ X \arrow[u, "p_j"] \arrow[ur, "p_i"'] & \end{tikzcd}$$

e tale che, $\forall (L, (\phi_i)_i)$ con la stessa proprietà, esiste $\phi : X \to L$ che fa commutare il diagramma

$$\begin{tikzcd} L \arrow[rr, "\phi"] \arrow[dr, "\phi_i"'] & & X \arrow[dl, "p_i"] \\ & X_i & \end{tikzcd}$$

Definizione. Un *sistema induttivo* di una categoria $\mathscr{C}$ è un sistema proiettivo nella categoria $\mathscr{C}^\circ$. Il suo *limite induttivo* è il colimite del diagramma nella categoria $\mathscr{C}$. Se $(X_i, (f_{ij})_{i \leq j})$ è un sistema induttivo, si denota con $\varinjlim X_i$ il limite induttivo.

Valgono i seguenti risultati:

Proposizione 1.2.1. Siano $\mathscr{C}$ una categoria, $(I, \leq)$ un insieme ordinato filtrante e $(X_i, (f_{ij})_{i \leq j})$ un sistema proiettivo. Allora un suo limite è dato dal funtore $\mathscr{C} \to \mathfrak{Set}$ che ad un oggetto T associa $\varprojlim \operatorname{Hom}(T, X_i)$.

Proposizione 1.2.2. Siano $\mathscr{C}$ una categoria e $(X_i, f_{ij})_I, (Y_i, g_{ij})_I$ due sistemi proiettivi che ammettono limiti proiettivi rispettivamente (X, p_i) e (Y, q_i). Sia $(h_i)_I$ un insieme di morfismi in $\mathscr{C}$ tali che $h_i : X_i \to Y_i$ e tali che $\forall i \leq j$ commuta il diagramma

$$\begin{tikzcd} X_j \arrow[r, "h_j"] \arrow[d, "f_{ij}"'] & Y_j \arrow[d, "g_{ij}"] \\ X_i \arrow[r, "h_i"'] & Y_i \end{tikzcd}$$

Allora esiste ed unico morfismo $h : X \to Y$ tale che $\forall i \in I$ commuta il diagramma

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "f_i"'] & Y \arrow[d, "g_i"] \\ X_i \arrow[r, "h_i"'] & Y_i \end{tikzcd}$$

In particolare, se tutti gli h_i sono isomorfismi, lo è anche h.

Proposizione 1.2.3. Sia $\mathfrak{U}$ un certo insieme universo e siano $\mathfrak{Gr}, \mathfrak{Top}, \mathfrak{TopGr}$ le categorie rispettivamente dei gruppi, degli spazi topologici e dei gruppi topologici definiti su $\mathfrak{U}$. Allora tutti i sistemi proiettivi indicizzati da un insieme filtrante I in $\mathfrak{U}$ ammettono limite proiettivo. Tali limiti commutano coi rispettivi funtori d'*oblio* verso $\mathfrak{Set}$. Inoltre, i limiti proiettivi di $\mathfrak{TopGr}$ commutano anche coi funtori d'*oblio* verso $\mathfrak{Gr}$ e $\mathfrak{Top}$.

Vale anche che in $\mathfrak{Top}$ un limite proiettivo di spazi compatti non vuoti è ancora compatto non vuoto.
Enunciamo un risultato sui limiti induttivi che tornerà utile più avanti.

Proposizione 1.2.4. Sia $((X_i)_I, (f_{i,j})_{i \leq j})$ un sistema induttivo nella categoria $\mathfrak{Set}$ e sia X il limite induttivo di tale sistema, ossia $X = \varinjlim X_i$. Allora si ha

$$X = {\left(\bigsqcup_I X_i\right)}\Big/_{\sim}$$

dove la relazione d'equivalenza $\sim$ è definita per $x_i \in X_i,\ x_j \in X_j$ con $i \leq j$ come

$$x_i \sim x_j \iff x_j = f_{i,j}(x_i)$$

La dimostrazione è omessa, ma basta dimostrare che l'insieme X munito delle applicazioni $f_i : X_i \hookrightarrow X$ definito come quoziente per una relazione d'equivalenza verifichi la proprietà universale.

Fissiamo ora $\mathscr{C}$ una categoria. Vogliamo definire una categoria avente per oggetti dei sistemi proiettivi in $\mathscr{C}$. Consideriamo quindi due sistemi proiettivi $X = ((X_i)_I, (f_{ij})_{i \leq j})$ e $Y = ((Y_h)_J, (g_{hk})_{h \leq k})$ in $\mathscr{C}$ e definiamo

$$\mathrm{Hom}(X, Y) = \varprojlim_j \varinjlim_i \mathrm{Hom}(X_i, Y_j)$$

Un elemento di $\mathrm{Hom}(X, Y)$ è quindi della forma $\phi = (\phi_j)$ con $\phi_j \in \varinjlim_i \mathrm{Hom}(X_i, Y_j)$. Dati $\phi = (\phi_j)_J \in Hom(X, Y)$ e $\psi = (\psi_k)_K \in \mathrm{Hom}(Y, Z)$, definiamo $\psi \circ \phi$ nel modo seguente: $\forall k \in K$ vediamo ψ_k come una coppia (j, ν) con $j \in J$ e $\nu \in \mathrm{Hom}(Y_j, Z_k)$, e definiamo $\omega_k = \nu \circ \phi_r \in \varinjlim_r \mathrm{Hom}(X_r, Z_k)$. Tale ω_k non dipende dalla scelta della coppia (j, ν). A questo punto è una facile verifica (e a detta di Douady, *sauf son effet soporifique*) mostrare che la costruzione appena fatta costituisce una categoria, che indichiamo con $\underset{\leftarrow}{\mathscr{C}}$, detta categoria dei *pro-oggetti*. Inoltre, definiamo la categoria opposta $\underset{\rightarrow}{\mathscr{C}}$ come la categoria tale che $(\underset{\rightarrow}{\mathscr{C}})^\circ = (\underset{\leftarrow}{\mathscr{C}^\circ})$. Facciamo solo tre osservazioni in merito:

- Ad un funtore $F : \mathscr{C} \to \mathscr{C}'$ corrisponde un funtore $\underset{\leftarrow}{F} : \underset{\leftarrow}{\mathscr{C}} \to \underset{\leftarrow}{\mathscr{C}'}$.
- Se F è un'equivalenza di categorie, lo è anche $\underset{\leftarrow}{F}$.
- La categoria $\mathscr{C}$ può essere vista come una sottocategoria piena di $\underset{\leftarrow}{\mathscr{C}}$.

Analizziamo ora il concetto di gruppo topologico.
Uno spazio topologico X è *totalmente discontinuo* se, $\forall x, y \in X$ distinti, esiste un aperto-chiuso U tale che $x \in U$ e $y \notin U$.

Definizione. Uno spazio topologico X è *spazio profinito* se soddisfa le seguenti condizioni (equivalenti):

i) X è compatto e totalmente discontinuo;

ii) X è omeomorfo al limite proiettivo di un sistema proiettivo di insiemi finiti discreti in $\mathfrak{Top}$.

Definizione. Uno gruppo topologico G è *gruppo profinito* se soddisfa le seguenti condizioni (equivalenti):

i) G come spazio topologico è profinito;

ii) G è limite proiettivo di gruppi finiti discreti in $\mathfrak{TopGr}$.

La categoria dei gruppi profiniti si denota con $\mathfrak{ProfGr}$ e ha per morfismi i morfismi tra gruppi topologici.

Sia G un gruppo profinito e G-$\mathfrak{FSet}$ la categoria degli insiemi finiti muniti di un'azione continua di G. Sia (G_i, f_{ij}) un sistema proiettivo di gruppi finiti e sia $(G_i$-$\mathfrak{FSet})$ il sistema induttivo di categorie corrispondente. Poniamo $G = \varprojlim G_i$.

Proposizione 1.2.5. La categoria G-$\mathfrak{FSet}$ è limite induttivo delle categorie G_i-$\mathfrak{FSet}$.

Per la dimostrazione di tale risultato si fa riferimento a [9, § 2.9.4].

Costruzione di un gruppo profinito

Vogliamo ora, partendo da un gruppo G, costruire il completamento profinito di G. Dato $(\mathcal{N}, \supseteq)$ insieme filtrante di sottogruppi distinti di indice finito di G, la famiglia $(G/N)_{N\in\mathcal{N}}$ munita delle proiezioni canoniche è un sistema profinito con limite proiettivo

$$\hat{G} = \varprojlim G/N$$

detto *completamento profinito* di G. Indico con η_G il morfismo canonico da G a $\hat{G}$.

In particolare, dati G e H gruppi con morfismo di gruppi $f : G \to H$, grazie a quanto detto precedente posso costruire uno ed unico morfismo di gruppi $G \to \hat{H}$ che commuta con $i : H \hookrightarrow \hat{H}$. Per la proprietà universale del completamento profinito posso allora costruire uno ed unico $\hat{f} : \hat{G} \to \hat{H}$ morfismo di gruppi topologici che fa commutare il diagramma

$$\begin{tikzcd} \hat{G} \arrow[r, "\hat{f}"] & \hat{H} \\ G \arrow[u, "\eta_G"] \arrow[r, "f"'] & H \arrow[u, "\eta_H"'] \end{tikzcd}$$

Siano G un gruppo profinito e (X_i) un sistema proiettivo in G-$\mathfrak{FSet}$: allora $X = \varprojlim X_i$ è uno spazio profinito su cui G agisce con continuità. Denotiamo con G-$\mathfrak{Prof}$ la categoria degli spazi profiniti su cui G agisce con continuità. Vale il seguente risultato, per la cui dimostrazione rimandiamo a [9, § 2.9.6].

Proposizione 1.2.6. Sia G un gruppo profinito. Il funtore che ad ogni sistema proiettivo nella categoria dei pro-oggetti $\overleftarrow{G\text{-}\mathfrak{FSet}}$ associa il suo limite proiettivo nella categoria G-$\mathfrak{Prof}$ è un'equivalenza di categorie.

Sia ora J un insieme finito. Sia $L(J)$ il gruppo libero costruito su J e $(X_i)_J$ l'insieme dei generatori canonici. Sia $\hat{L}(J)$ il completamento profinito di $L(J)$. Se $J \subset J'$, definiamo $\rho_{J,J'} : L(J') \to L(J)$ tale che $X_i \mapsto X_i$ se $i \in J$, $X_i \mapsto e$ altrimenti, dove e è l'elemento neutro del gruppo $L(J)$. Per passaggio al completamento, otteniamo $\hat{\rho}_{J,J'} : \hat{L}(J') \to \hat{L}(J)$.

Se I è un insieme qualsiasi e $\mathcal{J}$ l'insieme delle parti finite, allora $(\mathcal{J}, \subset)$ è filtrante e $((\hat{L}(J))_{J\in\mathcal{J}}, (\hat{\rho}_{J,J'})_{J\subset J'})$ è un sistema proiettivo con limite proiettivo

$$\hat{L}(I) = \varprojlim \hat{L}(J)$$

detto *gruppo profinito libero* costruito su I.

Vediamo come sono fatti gli elementi di $\hat{L}(I)$. Sia $J \subset I$ sottinsieme finito: definiamo la famiglia $(X_{i,J})_{i\in I} \subset \hat{L}(J)$ con $X_{i,J} = \rho_{J,J'}(X_i)$ se $i \in J$ e $X_{i,J} = e$ (elemento neutro) se $i \notin J$. Passando al limite proiettivo si ha la famiglia $(\hat{X}_{i,J})_i \subset \hat{L}(I)$.

Sia G un gruppo profinito. Diciamo che una famiglia $(x_i)_I$ di elementi di G tende all'elemento neutro e se, per ogni intorno U di e in G, l'insieme $\{i \ : \ x_i \notin U\}$ è finito. Se $G = \varprojlim G_\lambda$ con G_λ sottogruppi finiti, posta $\pi_\lambda : G \to G_\lambda$ la mappa canonica, dire che $(x_i)_i$ tende a e equivale a dire che la famiglia $(\pi_\lambda(x_i))_i$ è a supporto finito.

Proposizione 1.2.7. Sia I un insieme. Sia $\Phi : \overleftarrow{\mathfrak{ProfGr}} \to \mathfrak{Set}$ il funtore covariante che ad ogni gruppo profinito G associa l'insieme delle famiglie $(x_i)_I \subset G$ che tendono all'elemento neutro e di G. Allora:

i) il funtore Φ è rappresentato da $\hat{L}(I)$ munito della famiglia $(\hat{X}_i)_i$;

ii) siano L' un gruppo profinito e $(X'_i)_i \subset L'$ una famiglia che tende a e. Supponiamo che, $\forall G$ gruppo finito e $\forall (x_i)_I \subset G$ a supporto finito, esista uno ed unico omomorfismo continuo $f : L' \to G$ tale che $f(X'_i) = x_i$ per ogni i. Allora esiste uno ed unico isomorfismo $\hat{L}(I) \xrightarrow{\cong} L'$ tale che $\hat{X}_i \mapsto X'_i$.

Tale risultato, per la cui dimostrazione si rimanda a [9, § 6.4.1], servirà per dimostrare il risultato centrale del capitolo 4 (cf. Sez 4.1).

1.3 Rivestimenti topologici

Introduciamo ora il concetto di rivestimento, senza ridurci a spazi connessi ma per spazi topologici generici. D'ora in avanti, dato X uno spazio topologico e $x \in X$, indicheremo con $\mathcal{I}(x)$ l'insieme degli intorni di x in X.

Definizione. Dati due spazi topologici X e B, una funzione continua $\pi : X \to B$ è un *omeomorfismo locale* se $\forall x \in X$ esiste un intorno $U \in \mathcal{I}(x)$ tale che $\pi_{|_U} : U \to \pi(U)$ è un omeomorfismo. Inoltre, (X, π) è *proprio* su B se $\forall b \in B$ e $\forall (U_i)_I$ famiglia di aperti di X tale che $\pi^{-1}(b) \subset \bigcup_I U_i$ esistono $J \subset \mathcal{P}(I)$ finito e $V \in \mathcal{I}(b)$ tali che $\pi^{-1}(V) \subset \bigcup_J U_j$. Infine, (X, p) è *separato* su B se è T2 sulle fibre di p.

D'ora in avanti con (X, f) intenderemo $f : X \to \cdot$ surgettiva.

Definizione. (X, p) è un *rivestimento* di B se $\forall b \in B$ esistono $U \in \mathcal{I}(b)$, F spazio discreto e $\phi : p^{-1}(U) \to U \times F$ omeomorfismo che rende commutativo il diagramma

$$\begin{tikzcd} p^{-1}(U) \arrow[rr, "\phi"] \arrow[dr, "p"'] & & U \times F \arrow[dl, "\pi_U"] \\ & U & \end{tikzcd}$$

Osserviamo che la definizione data, sotto l'ipotesi di B connesso, è equivalente alla seguente:

Definizione. Dato B spazio topologico connesso, (X, p) è un *rivestimento* di B se $\forall b \in B$ esiste $V \in \mathcal{I}(b)$ aperto tale che $p^{-1}(V)$ è unione disgiunta di aperti $U_i \subset X$ per cui $p_{|_{U_i}} : U_i \to V$ è omeomorfismo.

Osservazione. I rivestimenti di B formano una sottocategoria piena $\mathfrak{Cov}_B \subset \mathfrak{Top}_B$.

Definizione. Dati (X, p) rivestimento di B e $b \in B$, il *grado* di X su b è il numero $\deg_b(X) = \#p^{-1}(b)$. Se B è non vuoto e il grado è costante al variare di $b \in B$, allora si parla di grado di X su B e si indica $\deg_B(X)$. Un rivestimento (X, p) di B è *finito* se $(\forall b \in B)$ $\deg_b(X)$ è finito.

Osservazione. Se lo spazio B è connesso, allora il grado delle fibre del rivestimento è costante, dunque si parla di grado del rivestimento.

Esempi. Vediamo alcuni esempi di rivestimenti:

- Data $\mathbb{e} : t \mapsto e^{it}$, $(\mathbb{R}, \mathbb{e})$ è un rivestimento di S^1 di grado ∞.
- (S^n, π) è rivestimento di grado 2 di $\mathbb{P}^n(\mathbb{R})$, con π la proiezione a quoziente per la relazione antipodale.

Fatto. Siano B localmente connesso, (X, p) e (Y, q) rivestimenti di B e $f : Y \to X$ morfismo di rivestimenti. Allora (Y, f) è rivestimento di X.

$$\begin{tikzcd} X \arrow[dr, "p"'] & & Y \arrow[ll, "f"'] \arrow[dl, "q"] \\ & B & \end{tikzcd}$$

Definizione. Uno spazio X è *semplicemente connesso* se è non vuoto e ogni suo rivestimento è triviale.

Ci chiediamo ora se la "composizione" di rivestimenti è ancora un rivestimento. Dati B, B' due spazi topologici, $f : B' \to B$ una mappa continua e X un rivestimento di B, indichiamo con $f^*(X) = B' \times_B X$ il rivestimento di B' ottenuto da X per *cambio di base* da B a B' tramite f.
Consideriamo B localmente connesso, (X, p) rivestimento di B e (Y, q) rivestimento di X. Siano $b \in B$ e $U \in \mathcal{I}(b)$ connesso trivializzante X (ossia, posta i l'inclusione di U in B, $i^*(X)$ è rivestimento triviale di U). Sia $(U_t)_F$ la famiglia delle componenti connesse di $X_{|_U} = p^{-1}(U)$.

$$\begin{tikzcd} Y \arrow[r, "q"] & X \arrow[r, "p"] & B \\ & i^*(X) \arrow[r, "p'"'] & U \arrow[u, "i"'] \end{tikzcd}$$

Per ogni $V \subset U$ aperto, definiamo $V_t = U_t \cap X_{|_V}$. Allora abbiamo che $(Y, p \circ q)$ è rivestimento di B all'intorno di b se e soltanto se esiste $V \in \mathcal{I}(b)$, $V \subset U$ aperto tale che $(\forall t \in F)$ V_t trivializza Y, ossia tale che, posta j l'inclusione di V in U, $(i \circ j)^*(Y)$ è rivestimento triviale di V_t.

$$\begin{tikzcd} Y \arrow[r, "q"] & X \arrow[r, "p"] & B \\ & & U \arrow[u, "i"'] \\ (i \circ j)^*(Y) \arrow[rr, "(p \circ q)'"'] & & V_t \arrow[u, "j"'] \end{tikzcd}$$

Corollario. Se X è rivestimento finito di B, allora ogni rivestimento Y di X è rivestimento di B. Se B è localmente semplicemente connesso, allora ogni rivestimento di un rivestimento di B è rivestimento di B.

Consideriamo ora la relazione $\sim$ di *omotopia* tra funzioni continue: quozientando $Mor(\mathfrak{Top})$ per tale relazione, si ottiene la categoria $\mathfrak{Homotop}$ avente per oggetti gli spazi topologici e per morfismi le classi di omotopia delle funzioni continue. Vale il risultato seguente, per la cui dimostrazione rimandiamo a [9, § 4.3.17]

Teorema. Siano B, B' spazi topologici, X rivestimento di B e $f, g : B' \to B$ continue. Se $f \sim g$, allora i rivestimenti $f^*(X)$ e $g^*(X)$ di B' sono isomorfi.

Definizione. Sia (B, b_0) uno spazio topologico con punto base b_0. Un rivestimento *puntato* (E, t_0) è un rivestimento (E, p) di B con $t_0 \in p^{-1}(b_0)$.
Dato (B, b_0) spazio puntato, se il funtore $\mathfrak{Cov}_B \to \mathfrak{Set}$ con $(X, p) \mapsto p^{-1}(b_0)$ è rappresentabile, un *rivestimento puntato universale* di (B, b_0) è una coppia (E, t_0) rappresentante tale funtore.

Equivalentemente, (E, t_0) è rivestimento puntato universale di (B, b_0) se e solo se $\forall (X, p) \in \mathfrak{Cov}_B$ e $\forall x \in p^{-1}(b_0)$ esiste un (unico) B-morfismo $f : E \to X$ tale che $f(t_0) = x$. Dunque un rivestimento puntato universale (E, t_0) di (B, b_0) è un *oggetto iniziale* per la categoria $\mathfrak{Cov}_{\circ B}$ dei rivestimenti puntati di (B, b_0), ossia $(\forall X \in \mathfrak{Cov}_{\circ B})$ $\mathrm{Hom}_{\mathfrak{Cov}_\circ}(E, X)$ è un singoletto.

Definizione. Sia (Y, p) un rivestimento di X. Un omeomorfismo $h : Y \to Y$ è *automorfismo* di rivestimenti se $p = p \circ h$.

L'insieme degli automorfismi di un rivestimento forma un gruppo munito con l'operazione di composizione, detto *gruppo degli automorfismi* (o *deck group*) e indicato con $\mathrm{Aut}(p)$.

Definizione. Un rivestimento (M, g) di X è *normale* (o *regolare* o *galoisiano*) se M è connesso, X è localmente connesso e localmente semplicemente connesso e $\mathrm{Aut}(p)$ agisce transitivamente su ogni fibra di p, ossia $(\forall a)$ $(\forall b, c \in p^{-1}(a))$ esiste $h \in \mathrm{Aut}(p)$ tale che $c = h(b)$.

Definizione. Un rivestimento (Y, b, p) di (X, a) è *puntato* se (Y, p) è un rivestimento di X tale che $p(b) = a$.

Un rivestimento $p : (Y, b) \to (X, a)$ induce l'omomorfismo di gruppi $p_* : \pi_1(Y, b) \to \pi_1(X, a)$. Nel caso di rivestimento puntato, tale omomorfismo è iniettivo. Due rivestimenti puntati di uno spazio X sono *equivalenti* se esiste un omeormofismo tra essi che commuta con le proiezioni su X e manda un punto base nell'altro punto base.

Definizione. Un rivestimento (Y_2, b_2) è *subordinato* a un rivestimento (Y_1, b_1) (entrambi di (X, a)) se esiste $h : Y_1 \to Y_2$ che commuta con le proiezioni su X.

Per rivestimenti subordinati, vale che Y_1 è subordinato a Y_2 se e solo se

$$p_*(\pi_1(Y_2)) \subset p_*(\pi_1(Y_1))$$

D'ora in avanti, se non diversamente specificato, supponiamo X localmente connesso e localmente semplicemente connesso e un suo rivestimento Y connesso.

Sia (Y,p) un rivestimento: supponiamo esista $a \in X$ per cui valga la proprietà $\mathcal{P}$:

$$\forall b, c \in p^{-1}(a),\ (Y,b) \text{ e } (Y,c) \text{ sono equivalenti come rivestimenti puntati di } (X,a)$$

Allora tale proprietà vale per ogni $a \in X$ e si ha che (Y,p) è normale. Viceversa, se (Y,p) è normale, la proprietà $\mathcal{P}$ vale per ogni $a \in X$.

Introduciamo ora un'altra nozione di rivestimento simile a quella di rivestimento subordinato.

Definizione. Sia (M,g) un rivestimento normale di X. Un rivestimento *intermedio* tra M e X è uno spazio Y con una mappa surgettiva $h_Y : M \to Y$ e una mappa $g_Y : Y \to X$ tali che $g = g_Y \circ h_Y$.

$$\begin{tikzcd} M \arrow[r, two heads, "h_Y"'] \arrow[rr, bend left, "g"] & Y \arrow[r, "g_Y"'] & X \end{tikzcd}$$

Due rivestimenti intermedi Y_1 e Y_2 tra (M,g) e X sono *equivalenti come sottorivestimenti* di (M,g) se esiste $h : Y_1 \to Y_2$ omeomorfismo che fa commutare il diagramma seguente

$$\begin{tikzcd} & Y_1 \arrow[dd, "h"'] \arrow[dr, "g_1"] & \\ M \arrow[ur, "h_1"] \arrow[rr, "g"] \arrow[dr, "h_2"'] & & X \\ & Y_2 \arrow[ur, "g_2"'] & \end{tikzcd}$$

Inoltre due sottorivestimenti di (M,g) sono *equivalenti come rivestimenti* di X se esiste $h : Y_1 \to Y_2$ omeomorfismo tale che $g_1 = g_2 \circ h$.

Capitolo 2

Teoria di Galois di Grothendieck

In questo capitolo, come in tutta la tesi, lavoriamo con algebre associative, commutative e con unità. Inoltre gli omomorfismi sono unitari. Salvo dove diversamente specificato, K sarà un campo. Indichiamo con $\mathfrak{Alg}_K$ la categoria delle K-algebre con morfismi gli omomorfismi unitari tra esse. Per le dimostrazioni omesse in questo capitolo, salvo dove diversamente specificato, è possibile consultare Douady, *Algèbre et théorie galoisiennes* [9, Cap V].

2.1 Estensioni di campi e algebre étale

In questa sezione estendiamo alcuni risultati della teoria dei campi ad un tipo di algebre, dette étale. Tali algebre ci permetteranno in seguito di riformulare la teoria di Galois in una forma categoriale e giocheranno un ruolo centrale nel risultato principe di questa trattazione.

Sia A una K-algebra. Per ogni $a \in A$ definiamo la valutazione in a

$$\hat{a} : \mathrm{Hom}_K(A, K) \to K$$

e chiamiamo *trasformazione di Gelfand* di A l'omomorfismo di K-algebre

$$\gamma : a \mapsto \hat{a}$$

Notiamo che se A è finita come K-algebra (ossia è un K-spazio vettoriale), allora γ è l'isomorfismo *lineare* canonico (tra K-spazi vettoriali, non tra K-algebre) tra A e il suo biduale $\hat{\hat{A}}$.

Definizione. Una K-algebra A finita di grado d è **diagonale** se (sono equivalenti):

- esiste X insieme finito tale che A è isomorfa a K^X;
- la trasformazione di Gelfand γ è un isomorfismo di algebre;
- $\forall a \in A \setminus \{0\}$ esiste $\zeta \in \mathrm{Hom}_K(A, K)$ tale che $\zeta(a) \neq 0$;
- $\#\,\mathrm{Hom}_K(A, K) = d$.

La proprietà *essere diagonale* passa alle sottoalgebre e ai quozienti di algebre diagonali. Inoltre, prodotto e prodotto tensore di algebre diagonali sono ancora algebre diagonali.

Lemma 2.1.1. Siano $\mathfrak{FSet}$ la categoria degli insiemi finiti e $\mathfrak{DAlg}_K$ la categoria delle K-algebre diagonali. Allora $\mathfrak{DAlg}_K$ è antiequivalente a $\mathfrak{FSet}$.

Dimostrazione. L'antiequivalenza è data dai funtori controvarianti

$$F : X \mapsto K^X \quad , \quad G : A \mapsto \mathrm{Hom}_K(A, K)$$

□

Da tale antiequivalenza segue che un'algebra diagonale ha un numero finito di sottoalgebre.

Definizione. Siano A una K-algebra finita e L/K un'estensione di campi. Diciamo che L **diagonalizza** A se $L \otimes_K A$ è una L-algebra diagonale.

Dalla definizione di algebra diagonale segue il seguente risultato.

Fatto. Condizione necessaria e sufficiente perchè L diagonalizzi A è che

$$\#\,\mathrm{Hom}_K(A, L) = [A : K]$$

Proposizione 2.1.2. Sia $P \in K[X]$ un polinomio di grado d e sia L/K un'estensione di campi. Allora L diagonalizza $K[X]/(P)$ se e solo se P ha d radici distinte in L.

Dimostrazione. Notiamo che $L \otimes_K K[X]/(P) \cong L[X]/(P)$ e $[L[X]/(P) : L] = d$. Inoltre, se P ha d radici distinte il L, si ha $\#\,\mathrm{Hom}_L(L[X]/(P), L) = d$. L'osservazione precedente conclude. □

Diamo ora una definizione che in qualche modo estende alle algebre la definizione di *estensione di campi di Galois.*

Definizione. Sia Ω una chiusura algebrica di K. Una K-algebra finita A è **ètale** se (sono equivalenti):

- esiste un'estensione L/K che diagonalizza A;
- esiste un'estensione finita L/K che diagonalizza A;
- Ω diagonalizza A.

In particolare, dalla proposizione precedente segue che, dato $P \in K[X]$, sono equivalenti:

- $K[X]/(P)$ è una K-algebra étale;
- le radici di P in Ω sono tutte distinte;
- $\gcd(P, P') = 1$;
- il discriminate Δ_P è non nullo.

In tal caso, il polinomio P è detto *separabile*. Una K-algebra è detta **separabile** se ogni suo elemento ammette polinomio minimo separabile.

Definizione. Sia A una K-algebra. Definiamo **chiusura separabile** di K in A la sottoalgebra

$$A_s := \{a \in A \mid a \text{ separabile su } K\}$$

Come per le algebre diagonali, la proprietà *essere étale* passa alle sottoalgebre e ai quozienti di algebre étale, e prodotto e prodotto tensore di algebre étale sono ancora algebre étale.
Vale inoltre il seguente risultato.

Fatto. Condizione necessaria e sufficiente perchè un'algebra sia étale è che sia finita e separabile.

Enunciamo ora alcuni risultati delle algebre étale collegati alla teoria dei campi:

- Se L/K è un'estensione étale e A è un'algebra étale su L, allora lo è anche su K.
- Sia $A = K(\alpha)$ estensione finita e sia $P \in K[X]$ irriducibile tale che $A \cong K[X]/(P)$. Allora A non è étale su $K \iff \mathit{char} K = p \neq 0$ e $P \in K[X^p]$.

Definizione. Un campo K è **perfetto** se ogni sua estensione finita è separabile (e quindi étale), o equivalentemente se, posta $\mathit{char} K = p$, si ha $p = 0$ oppure l'endomorfismo di Frobenius $x \mapsto x^p$ di K è surgettivo.

Definizione. Una K-algebra è **ridotta** se non ha nilpotenti non nulli.

Vediamo ora due risultati relativi alle algebre étale ridotte.

Proposizione 2.1.3. Sia A una K-algebra finita.

i) Se K è perfetto, A è étale $\iff$ A è ridotta.

ii) Se $(x_1 \dots x_r)$ genera A come K-algebra e $P_1 \dots P_r$ sono i relativi polinomi minimi, allora A è étale $\iff$ $\forall i \ \gcd(P_i, P_i') = 1$.

iii) Se $charK = p \neq 0$ e A è un'estensione, allora A è étale $\iff$ $\forall i \ P_i \notin K[X^p]$.

Corollario 2.1.4. Sia K un campo perfetto. Il prodotto tensore di due K-algebre finite ridotte è una K-algebra finita ridotta. In particolare, il prodotto tensore di due estensioni finite su K è una K-algebra ridotta.

Enunciamo ora un'estensione alle algebre étale del *teorema dell'elemento primitivo* della teoria dei campi.

Teorema 2.1.5. Sia K un campo infinito. Ogni K-algebra étale è semplice, ossia ammette un unico generatore, detto *elemento minimo*.

Dimostrazione.

a) Vediamo che un'algebra étale A ha un numero finito di sottoalgebre. Sia L un'estensione di K tale che $L \otimes_K A$ sia diagonale. Per ogni sottoalgebra B di A, $L \otimes_K B$ è una sottoalgebra di $L \otimes_K A$ e vale $B = A \cap (L \otimes_K B)$. Allora la mappa che ad ogni sottoalgebra B di A associa la sottolagebra $L \otimes_K B$ di $L \otimes_K A$ è iniettiva. Ma un'algebra diagonale ha un numero finito di sottoalgebre. Segue che anche A ha un numero finito di sottoalgebre.

b) Sia E un K-spazio vettoriale di dimensione finita e sia (F_i) una famiglia finita di sottospazi propri di E. Dimostriamo che $\bigcup F_i \neq E$. Possiamo estendere ciascun sottospazio F_i ad un iperpiano H_i definito da un'equazione $h_i = 0$. Supponiamo $E = K^n$: allora gli h_i sono polinomi omogenei non nulli in n variabili di grado 1. Allora $h = \prod_i h_i$ è non nullo. Poichè K è infinito, la mappa polinomiale $h : K^n \to K$ non è nulla ed esiste $x \in K^n$ tale che $h(x) \neq 0$, ossia $x \notin \prod_i H_i$.

c) Sia ora A una K-algebra étale: essa è finita e ha un numero finito di sottoalgebre proprie $A_1, \dots, A_r$ (punto a)). Per il punto b) sappiamo che $\bigcup_{i=1}^r A_i \neq A$. Sia $x \in A \setminus \bigcup_{i=1}^r A_i$. Allora la sottoalgebra generata da x non è una sottoalgebra propria, dunque x genera A.

□

Notiamo che nel caso di estensioni di campi di K, il risultato è vero anche per K finito. Per una dimostrazione di tale caso, è possibile consultare *Algebra* di S. Bosch [8, § 3.6.12].

2.2 Teoria di Galois finita

In questa sezione diamo una breve review della teoria di Galois finita in termini di teoria dei campi, per poi presentare la teoria di Galois in chiave categoriale, ricorrendo alle algebre étale, e arrivare a ottenere un'antiequivalenza tra la categoria $\mathfrak{D}_L$ delle K-algebre finite diagonalizzate da un'estensione di Galois L di K e la categoria $\mathrm{Gal}(L/K)$-$\mathfrak{FSet}$ *degli insiemi finiti su cui è definita un'azione del gruppo di Galois* $\mathrm{Gal}(L/K)$*.*

Dato F un campo, indichiamo con $\overline{F}$ una sua chiusura algebrica.

Definizione. Un'estensione algebrica L/K è **normale** se per ogni omomorfismo di campi $\sigma : L \to \overline{L}$ tale che $\phi|_K = id$ vale $\sigma(L) = L$. Un'estensione algebrica L/K è **separabile** se per ogni $\alpha \in L$ il suo polinomio minimo μ_α su K ha tutte radici distinte in $\overline{K}$. Un'estensione algebrica L/K è **di Galois** se è normale e separabile e in tal caso si indica il gruppo di automorfismi dell'estensione con $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Ricordiamo inoltre che, dati due campi L, F contenuti in uno stesso campo algebricamente chiuso Ω, il loro *composito* (o prodotto) LF è il campo generato dalle due estensioni, ossia

$$LF = L(F) = F(L) = \bigcap_{L,F \subset E \subset \Omega} E$$

Enunciamo ora un risultato centrale della teoria di Galois, dovuto a Emil Artin, utile per dimostrare il *teorema fondamentale della teoria di Galois.*

Lemma 2.2.1 (Lemma di Artin)**.** Sia L un campo e sia G un sottogruppo di $\mathrm{Aut}(L)$. Sia $K = \mathrm{Fix}_G(L)$. Allora:

1. Se G è finito, l'estensione L/K è di Galois finita e $G = \mathrm{Gal}(L/K)$.

2. Se G è infinito e l'estensione L/K è algebrica, allora L/K è di Galois infinita e $G < \mathrm{Gal}(L/K)$.

Per la dimostrazione di questo risultato, e del successivo, è possibile consultare *Algebra* di S. Bosch [8, § 4.1.4 , § 4.1.6]. Indichiamo con $H \triangleleft G$ un sottogruppo normale H del gruppo G.

Teorema 2.2.2 (Corrispondenza di Galois - caso finito)**.** Sia L/K un'estensione di Galois e sia $G = \mathrm{Gal}(L/K)$ il suo gruppo di Galois. Allora esistone due mappe

$$\begin{tikzcd} \{H \mid H < G\} \arrow[rr, bend left, "\phi"] & & \{F \mid K \subset F \subset L\} \arrow[ll, bend left, "\psi"] \end{tikzcd}$$

$$\phi(H) = \mathrm{Fix}_H(L)\ ,\ \psi(F) = \mathrm{Gal}(L/F)$$

tali che $\phi \circ \psi = id$, ossia tali che ψ è iniettiva e ϕ è surgettiva. Inoltre, F/K è di Galois $\iff \mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K)$, e in tal caso

$$\mathrm{Gal}(F/K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)}$$

Se G è finito, vale anche $\psi \circ \phi = id$ (ossia ψ e ϕ sono bigettive) e

$$H \triangleleft G \iff \mathrm{Fix}_H(L)/K \text{ è di Galois}$$

Torniamo ora a ragionare in termini di algebre étale.

Definizione. Un'estensione finita L di K è **di Galois** se L diagonalizza se stessa. Se L/K è di Galois, il suo **gruppo di Galois** è il gruppo $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Ricordiamo che L diagonalizza se stessa $\iff \#\,\mathrm{Hom}_K(L, L) = [L : K]$.

Osservazione. Notiamo che se L/K è di Galois e $K \subset A \subset L$ è una torre di campi, allora L diagonalizza A su K e L/A è di Galois (vista come A-algebra).

Vediamo ora una caratterizzazione delle estensioni di Galois finite di un campo K. Sia Ω una chiusura algebrica di K contenente un'estensione $L \supset K$ finita.

Teorema 2.2.3. Sono equivalenti:

i) L/K è di Galois;

ii) $\#\,\mathrm{Aut}_K L = [L : K]$;

iii) L è étale su K e $\forall \phi \in \mathrm{Aut}_K(\Omega)$ si ha $\phi(L) = L$;

iv) Se $G = \mathrm{Aut}_K(L)$, allora $\mathrm{Fix}_G(L) = K$;

v) $\forall x \in L$, le radici in Ω del polinomio minimo di x sono semplici e appartengono ad L.

Corollario 2.2.4. Siano L, L' due estensioni di Galois di K contenute nella stessa chiusura algebrica Ω. Allora il prodotto di campi LL' è di Galois su K.

Corollario 2.2.5. Siano $K \subset L' \subset L \subset \Omega$ con L/K e L'/K di Galois finite. Siano $G = \mathrm{Gal}(L/K)$, $G' = \mathrm{Gal}(L'/K)$ e $H = \mathrm{Gal}(L/L')$. Allora

$$H \triangleleft G \quad \text{e} \quad G' \cong {}^{G}\!/\!_{H}$$

Ricordiamo che un'estensione di K è normale *se e solo se* campo di spezzamento di una famiglia di polinomi in $K[X]$. Abbiamo il seguente risultato che collega le algebre étale e le estensioni di Galois.

Proposizione 2.2.6. Sia A una K-algebra étale. Allora esiste un'estensione di Galois L/K finita tale che L diagonalizza A.

Dimostrazione. Sia Ω una chiusura algebrica di K e siano $x_1, \ldots, x_r$ dei generatori di A come algebra su K. Per ogni i, denotiamo con P_i il polinomio minimo di x_i su K e con L_i il campo di spezzamento su K in Ω di P_i. Per ogni i, L_i diagonalizza la sottoalgebra A_i di A generata da x_i. Inoltre, il composito di campi $L = L_1 \ldots L_r$ diagonalizza ogni A_i, dunque L diagonalizza A, ed è un'estensione finita in quanto composito di estensioni finite.
Vediamo che l'estensione L/K è di Galois. Poichè A è étale, le radici di ogni P_i sono semplici, quindi L è étale. Ciascun automorfismo di Ω permuta tra loro le radici di ogni P_i, dunque fissa L, ossia L è di Galois. □

Un'antiequivalenza di categorie

Consideriamo ora un'estensione di Galois finita L/K e una K-algebra finita A diagonalizzata da L. Poniamo $G = \mathrm{Aut}_K(L)$ e $X = \mathrm{Hom}_K(A, L)$: poichè L diagonalizza A, si ha $\#X = [A : K]$. Inoltre, $L \otimes_K A$ è diagonale.
Identifichiamo $X = \mathrm{Hom}_L(L \otimes_K A, L)$. Consideriamo l'azione di G su X data da

$$\forall g \in G \ , \ \forall \zeta \in X, \quad g \cdot \zeta := g \circ \zeta$$

Sia γ la trasformazione di Gelfand sulla L-algebra $L \otimes_K A$

$$\gamma : L \otimes_K A \longrightarrow L^X$$

con $\gamma : t \mapsto \hat{t}$ tale che $\hat{t}(\zeta) = \zeta(t)$ per $\zeta \in X$.
Se $t = \lambda \otimes a$, allora $\gamma(\lambda \otimes a) = \widehat{\lambda \otimes a}(\zeta) = \zeta(\lambda \otimes a) = \lambda\zeta(a)$.
Per definizione G agisce su L: possiamo estendere l'azione su $L \otimes_K A$ ponendo

$$g_* : (\lambda \otimes a) \mapsto g(\lambda) \otimes a$$

Poichè $L \otimes_K A$ è diagonale, la trasformazione di Gelfand γ è un isomorfismo. Allora l'azione di G su $L \otimes_K A$ induce un'azione di G su L^X che denotiamo con

$$g_\perp : f \mapsto g \perp f$$

per ogni $g \in G, \ f \in L^X$.
Abbiamo dunque il seguente diagramma commutativo

$$\begin{tikzcd}
L \otimes_K A \arrow[r, "\gamma"] \arrow[d, "g_* := g \otimes \mathbb{1}_A"'] & L^X \arrow[d, "g_\perp"] \\
L \otimes_K A \arrow[r, "\gamma"'] & L^X
\end{tikzcd}$$

Vediamo che la legge $\perp$: $G \times L^X \to L^X$ è data dalla formula

$$(g \perp f)(\zeta) = g(f(g^{-1} \circ \zeta))$$

Dati $\zeta \in X$ e $g \in G$, consideriamo l'omomorfismo di K-algebre

$$\begin{array}{cccc} \phi : & L^X & \longrightarrow & L \\ & f & \mapsto & (g \perp f)(\zeta) \end{array}$$

Il kernel di ϕ è un ideale massimale $\mathfrak{m}_\eta$ di L^X, con $\eta \in X$. Nel diagramma sopra, la mappa g_* è g-lineare, mentre γ è L-lineare: allora $g_\perp$ è g-lineare, ossia $\forall \lambda \in L$, $\forall f \in L^X$ vale $\phi(\lambda f) = g(\lambda)\phi(f)$. Per la massimalità di $\mathfrak{m}_\eta$, ogni $f \in L^X$ è del tipo $f = f(\eta)\cdot 1 + f_1$, per un certo $f_1 \in \mathfrak{m}_\eta$. Segue che $\phi(f) = g(f(\eta))$. Vogliamo dunque determinare η. Dati $\lambda \in L$ e $a \in A$, per definizione di $\perp$ si ha

$$(g \perp (\widehat{\lambda \otimes a}))(\zeta) = (\widehat{g(\lambda) \otimes a})(\zeta) = g(\lambda) \cdot \zeta(a)$$

D'altra parte

$$(g \perp (\widehat{\lambda \otimes a})(\zeta) = \phi(\widehat{\lambda \otimes a}) = g(\widehat{\lambda \otimes a})(\eta) = g(\lambda \cdot \eta(a)) = g(\lambda) \cdot g(\eta(a))$$

e ponendo $\lambda = 1$ si ha $\zeta(a) = g(\eta(a))$, da cui $\eta = g^{-1} \circ \zeta$, dunque

$$(g \perp f)(\zeta) = \phi(f) = g(f(\eta)) = g(f(g^{-1} \circ \zeta))$$

Fatte queste premesse e fissati L/K di Galois finita e $G = \mathrm{Aut}_K(L)$, vogliamo arrivare ad un'antiequivalenza di categorie tra la categoria G-$\mathfrak{FSet}$ degli insiemi finiti su cui è definita un'azione di G e la categoria $\mathfrak{D}_L$ delle K-algebre finite diagonalizzate da L.

Sia $A \in \mathfrak{D}_L$. Denotiamo con $S(A) = \mathrm{Hom}_K(A, L)$: allora G agisce su $S(A)$ tramite $g \cdot f = g \circ f$. Definiamo quindi un funtore controvariante

$$\begin{array}{cccc} S : & \mathfrak{D}_L & \longrightarrow & G\text{-}\mathfrak{FSet} \\ & A & \mapsto & S(A) \end{array}$$

Dato $f : A \to B$ omomorfismo di K-algebre, si ha la mappa tra G-insiemi $f^* : S(B) \to S(A)$ definita da $f^*(\eta) = \eta \circ f$.

Teorema 2.2.7. Il funtore $S : \mathfrak{D}_L \to \mathrm{Gal}(L/K)\text{-}\mathfrak{FSet}$ è un'antiequivalenza di categorie.

La dimostrazione di questo teorema segue agilmente dalle due seguenti proposizioni.

Proposizione 2.2.8 (Fedeltà piena)**.** Siano $A, B \in \mathfrak{D}_L$. Allora $\forall \phi \in Hom_G(S(B), S(A))$ esiste $f \in \mathrm{Hom}_K(A, B)$ tale che $f^* = \phi$.

Dimostrazione.

a) $\forall A \in \mathfrak{D}_L$ vale $\mathrm{Fix}_G(L \otimes_K A) = A$: in quanto K-spazio vettoriale, possiamo identificare A con K^d. Allora come L-spazi vettoriali, $L \otimes_K K^d \cong L^d$. Poichè G agisce sulle singole componenti di L^d e L/K è di Galois, si ha $\mathrm{Fix}_G(L) = K \implies \mathrm{Fix}_G(L^d) = K^d$.

b) Sia $\phi : S(B) \to S(A)$ un G-morfismo: ad esso corrisponde un morfismo di L-algebre $\phi^* : L^{S(A)} \to L^{S(B)}$ definito da $\phi^*(h) = h \circ \phi$. L'omomorfismo ϕ^* è compatibile con l'azione $\perp$ di G, ossia $\phi^*(g \perp h) = g \perp \phi^*(h)$: infatti, dato $\zeta \in S(A)$, si ha

$$\begin{aligned}\phi^*(g \perp h)(\zeta) &= (g \perp h)(\phi(\zeta)) = g(h(g^{-1} \circ \phi(\zeta))) = \\ &= g(h(\phi(g^{-1} \circ \zeta))) = (g \perp (h \circ \phi))(\zeta) = \\ &= (g \perp \phi^*(h))(\zeta)\end{aligned}$$

Poichè L diagonalizza A, le trasformazioni di Gelfand

$$\gamma_A : L \otimes_K A \to L^{S(A)} \quad , \quad \gamma_B : L \otimes_K B \to L^{S(B)}$$

sono isomorfismi, quindi esiste un unico omomorfismo $\phi^{\otimes} : L \otimes_K A \to L \otimes_K B$ che fa commutare il diagramma

$$\begin{tikzcd} L \otimes_K A \arrow[r, "\gamma_A"] \arrow[d, "\phi^{\otimes}"'] & L^{S(A)} \arrow[d, "\phi^*"] \\ L \otimes_K B \arrow[r, "\gamma_B"'] & L^S(B) \end{tikzcd}$$

Tale omomorfismo è compatibile con le azioni di G, quindi (grazie al punto (a)) $\phi^{\otimes}$ induce un omomorfismo di K-algebre

$$f : A = \mathrm{Fix}_G(L \otimes_K A) \to B = \mathrm{Fix}_G(L \otimes B)$$

da cui otteniamo il diagramma commutativo

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[d, "f"'] & L \otimes_K A \arrow[r, "\gamma_A"] \arrow[d, "\phi^{\otimes}"'] & L^{S(A)} \arrow[d, "\phi^*"] \\
B \arrow[r, "i_B"'] & L \otimes_K B \arrow[r, "\gamma_B"'] & L^{S(B)}
\end{tikzcd}$$

con $i_A : A \hookrightarrow L \otimes_K A$ e $i_B : B \hookrightarrow L \otimes_K B$ le immersioni canoniche.
Mostriamo ora che $f^* : S(B) \to S(A)$ coincide con ϕ. Basta verificare che

$$\forall \eta \in \mathrm{Hom}_K(B, L), \ \ \eta \circ f = \phi(\eta)$$

Sia $\delta_\eta : L^{S(B)} \to L$ l'omomorfismo definito da $\delta_\eta(h) = h(\eta)$: per definizione della trasformazione di Gelfand γ_B, si ha $\eta = \delta_\eta \circ \gamma_B \circ i_B$.

$$\begin{aligned}
\eta \circ f = \delta_\eta \circ \gamma_B \circ i_B \circ f = \delta_\eta \circ \gamma_B \circ \phi^{\otimes} \circ i_A = \\
= \delta_\eta \circ \phi^* \circ \gamma_A \circ i_A = \delta_{\phi(\eta)} \circ \gamma_A \circ i_A = \\
= \phi(\eta)
\end{aligned}$$

□

Proposizione 2.2.9 (Surgettività essenziale)**.** Ogni G-insieme finito è isomorfo ad un G-insieme della forma $S(A)$ per un qualche $A \in \mathfrak{D}_L$.

Dimostrazione.

a) Vediamo prima che, dati $H < G$ e $F = \mathrm{Fix}_H(L)$, sappiamo determinare $S(F)$. La restrizione $\rho : G \to \mathrm{Hom}_K(F, L)$ è surgettiva: infatti, preso L in una chiusura algebrica Ω di K, dalla teoria dei campi sappiamo che ogni K-omomorfismo $F \to L$ si prolunga ad un omomorfismo $L \to \Omega$ (Bosch, *Algebra*, [8, § 3.4.9]), che induce un automorfismo di L (in quanto L/K è di Galois). Siano $f, g \in G = \mathrm{Aut}_K(L)$: allora si ha $\rho(f) = \rho(g)$ se e solo se l'elemento $h \in G$ definito da $g = f \circ h$ appartiene a $\mathrm{Aut}_F(L)$. Per il lemma di Artin (lemma 2.2.1), si ha $\mathrm{Aut}_F(L) = H$, da cui $S(F) = \mathrm{Hom}_K(F, L)$ s'identifica con l'insieme delle classi laterali $G/H = \{fH\}_{f \in G}$. Tale identificazione è compatibile con l'azione a sinistra di G.

b) Siano $A, B \in \mathfrak{D}_L$. Allora si ha $S(A \times B) = S(A) \sqcup S(B)$: infatti valgono

$$L \otimes_K A = L^{S(A)} \ \ , \ \ L \otimes_K L^{S(B)}$$

$$L \otimes_K (A \times B) = (L \otimes_K A) \times (L \otimes_K B) = L^{S(A)} \times L^{S(B)} = L^{S(A) \sqcup S(B)}$$

da cui $S(A \times B) = \mathrm{Hom}_L(L^{S(A) \sqcup S(B)}, L) = S(A) \sqcup S(B)$.

c) Prima di concludere, ci serve il seguente fatto:

Fatto. Ogni G-insieme finito è isomorfo a $\bigsqcup_I G/H_i$ con $\{H_i\}_I$ una famiglia finita di sottogruppi di G.

Dunque, dato X un G-insieme finito, sappiamo che

$$X = \bigsqcup_I G/H_i \overset{(a)}{=} \bigsqcup_I S(\mathrm{Fix}_{H_i}(L)) \overset{(b)}{=} S(\prod_I \mathrm{Fix}_{H_i}(L))$$

dove $\prod_I \mathrm{Fix}_{H_i}(L) \in \mathfrak{D}_L$.

$\square$

2.3 Teoria di Galois infinita

In questa ultima sezione estendiamo la teoria di Galois appena vista al caso infinito. A tal scopo riprendiamo il concetto di gruppo profinito munendo il gruppo $\mathbb{G} = \mathrm{Aut}_K(\Omega)$ di una topologia, detta topologia di Krull, per poi studiare le estensioni L/K di Galois infinite ed estendere l'antiequivalenza vista precedentemente alle categorie $\mathfrak{A}$ delle K-algebre separabili e $\mathbb{G}$-$\mathfrak{Prof}$ degli spazi profiniti su cui $\mathbb{G}$ opera con continuità.

Fissiamo Ω una chiusura algebrica di K e indichiamo con Ω_s la chiusura separabile di K in Ω: allora Ω_s/K è un'estensione di Galois infinita. Sia $\mathbb{G}$ il gruppo $\mathrm{Aut}_K(\Omega)$ degli automorfismi di Ω che lasciano fisso K.

Proposizione 2.3.1. $\mathbb{G} = \mathrm{Aut}_K(\Omega_s)$.

Dimostrazione. Dalla teoria dei campi sappiamo che ogni automorfismo di Ω_s è prolungabile ad un automorfismo di Ω. Inoltre, poichè Ω è un'estensione puramente inseparabile di Ω_s, ogni automorfismo di Ω_s ha un unico prolungamento. $\square$

Consideriamo ora l'insieme $\mathscr{E}$ delle estensioni di Galois finite di K contenute in Ω, munito dell'ordinamento di inclusione. $\mathscr{E}$ è un insieme *filtrante*, ossia date due estensioni di Galois finite, esiste un'estensione di Galois finita che contiene il loro composito: infatti il composito di due estensioni finite di Galois è ancora étale e stabile per $\mathbb{G}$, quindi di Galois.

Dati $E \subset F \in \mathscr{E}$, ogni K-automorfismo di F induce un K-automorfismo di E, per cui è ben definito l'omomorfismo di restrizione

$$\rho_E^F : \mathrm{Aut}_K(F) \to \mathrm{Aut}_K(E)$$

Notiamo che $\Omega_s = \bigcup_{\mathscr{E}} E$, da cui segue che

$$\mathbb{G} = \mathrm{Aut}_K(\Omega_s) = \varprojlim \mathrm{Aut}_K(E)$$

Poniamo dunque su $\mathbb{G}$ una topologia, detta *topologia di Krull*, ottenuta tramite la precedente identificazione dalla topologia del limite proiettivo.

Proviamo ora a esplicitare tale topologia su $\mathbb{G}$. Lo studio che faremo (con i relativi risultati) è identico se al posto di Ω_s/K si considera una qualsiasi estensione L/K di Galois infinita. Consideriamo la famiglia

$$\mathcal{L} = \{L_i \mid K \subset L_i \subset \Omega_s,\ L_i/K \text{ di Galois finita}\}$$

Allora $\Omega_s = \bigcup_{i \in I} L_i$ e per ogni i si ha la restrizione

$$\begin{array}{cccc} \cdot|_{L_i} & \mathbb{G} & \longrightarrow & \mathrm{Gal}\left({}^{L_i}\!/\!_{K}\right) \\ & \sigma & \longmapsto & \sigma_i = \sigma|_{L_i} \end{array}$$

avente come nucleo $\mathrm{Ker}(\cdot|_{L_i}) = \mathrm{Gal}(\Omega_s/L_i) \lhd \mathbb{G}$. Possiamo considerare la mappa

$$\begin{array}{cccc} \rho\colon & \mathbb{G} & \longrightarrow & \prod_I \mathrm{Gal}(L_i/K) \\ & \sigma & \longmapsto & (\sigma_i)_{i \in I} \end{array}$$

L'immagine di ρ sono le successioni coerenti, ossia quelle tali che se $L_i \subset L_j$, allora $\sigma_j|_{L_i} = \sigma_i$. Infatti, per la coerenza, è ben definita l'estensione dei $\sigma_i \in \mathrm{Gal}(L_i/K)$ ad un $\sigma \in \mathbb{G}$. Inoltre, ρ è iniettiva: se $\rho(\sigma) = (id)_I$, allora per ogni $\alpha \in L$ esiste un indice i tale che $\sigma(\alpha) = \sigma_i(\alpha) = \alpha$, ossia $\sigma = id$.

Tramite ρ, possiamo dotare $\mathbb{G}$ della topologia di sottospazio. Allora la topologia di Krull su $\mathbb{G}$ è data da

$$\mathcal{K} = \{\rho^{-1}(\mathcal{U}_i) \mid \mathcal{U}_i \subset \prod_I \mathrm{Gal}(L_i/K) \text{ aperto}\}$$

Vediamo quindi chi sono gli aperti in $\prod_I \mathrm{Gal}(L_i/K)$: una pre-base è data dagli $\mathcal{U}_i = \prod_j V_j$ con

$$V_j = \mathrm{Gal}(L_j/K) \text{ se } i \neq j,\ V_i = \{\sigma_i\}$$

Dunque, gli aperti di $\mathbb{G}$ sono tutti della forma

$$\rho^{-1}(\prod_j V_j) = (\cdot|_{L_i})^{-1}(\sigma_i) = \tilde{\sigma_i}\,\mathrm{Gal}(L/L_i)$$

(con $\tilde{\sigma_i}$ l'estensione di σ_i a L), ossia sono le classi laterali dei nuclei delle restrizioni $\cdot|_{L_i}$. Allora una pre-base della topologia di Krull su $\mathbb{G}$ è

$$\{\sigma\,\mathrm{Gal}(L/L_i) \mid \sigma \in \mathbb{G}\}_{i \in I}$$

L'intersezione di due aperti della pre-base può essere del tipo

$$\tilde{\sigma_i}\,\mathrm{Gal}(L/L_i) \cap \tilde{\sigma_j}\,\mathrm{Gal}(L/L_j) = \emptyset$$

oppure

$$\tilde{\sigma_i}\,\mathrm{Gal}(L/L_i) \cap \tilde{\sigma_j}\,\mathrm{Gal}(L/L_j) = \bigcup_{r=1}^{n} \tilde{\sigma_r}\,\mathrm{Gal}(L/L_k)$$

con $L_k \subset L_i L_j$. Si osservi che $\sigma_i \in \mathrm{Gal}(L_i/K)$ non ha un'unica estensione a L, ma si estende a $\tilde{\sigma_{i_1}}, \dots, \tilde{\sigma_{i_m}}$.

Proposizione 2.3.2. $(\mathbb{G}, \mathcal{K})$ è un gruppo topologico.

Dimostrazione. Dobbiamo mostrare che le mappe

$$m : (\sigma, \tau) \mapsto \sigma\tau \qquad\qquad \gamma : \sigma \mapsto \sigma^{-1}$$

sono continue. Devo verificare che le controimmagini di aperti tramite le mappe m e γ sono aperti.

- Sia $\sigma\tau\,\mathrm{Gal}(L/L_k)$ un aperto in $\mathbb{G}$. Considero $\mathcal{U}_\sigma = \sigma\,\mathrm{Gal}(L/L_k)$ e $\mathcal{U}_\tau\,\mathrm{Gal}(L/L_k)$. Ma $m(\mathcal{U}_\sigma, \mathcal{U}_\tau) = \mathcal{U}_\sigma \mathcal{U}_\tau \overset{(*)}{=} \mathcal{U}_{\sigma\tau}$, dove $\overset{(*)}{=}$ é dovuto all'operazione tra classi laterali. Allora $m^{-1}(\sigma\tau\,\mathrm{Gal}(L/L_k)) = \sigma \times \mathcal{U}_\tau$, che é aperto.

- Sia $\sigma^{-1}\,\mathrm{Gal}(L/L_k)$ un aperto in $\mathbb{G}$ e con considerazioni analoghe si ha

  $$\gamma^{-1}(\sigma^{-1}\,\mathrm{Gal}(L/L_k)) = \sigma\,\mathrm{Gal}(L/L_k)$$

  che é aperto.

$\square$

Notiamo che una volta definiti gli intorni di 1, gli intorni di $\sigma \in \mathbb{G}$ sono definiti dalle traslazioni degli intorni di 1. Indichiamo con $\mathcal{I}(x) = \{\mathcal{U} \subset \mathbb{G} \text{ intorno di } x\}$. Allora una base di $\mathcal{I}(1)$ è $\{\mathrm{Gal}(L/L_i)\}_{i \in I}$, per cui dato $\sigma \in \mathbb{G}$ si ha

$$\mathcal{I}(\sigma) = \{\sigma\,\mathrm{Gal}(L/L_i)\}_{i \in I}$$

Osservazione. In ogni gruppo topologico, i sottogruppi aperti sono anche chiusi: infatti se $H < G$ é aperto, allora gH è aperto per ogni $g \in G$; ma allora $G = \bigcup_g gH$ implica $G \setminus H = \bigcup_{g \neq id} gH$, che é aperto in quanto unione di aperti. Ne segue che H è anche chiuso. In particolare, i $\mathrm{Gal}(L/L_i)$ sono aperti e chiusi in $\mathbb{G}$.

Ricordiamo che uno spazio topologico è *totalmente sconnesso* se le sue componenti connesse sono tutte e sole i punti. Vale il seguente risultato, per la cui dimostrazione si rimanda a Bosch, *Algebra* [8, § 4.2.2].

Lemma 2.3.3. $(\mathbb{G}, \mathcal{K})$ è di Hausdorff, compatto e totalmente sconnesso.

Dato H un sottogruppo di un gruppo profinito G, indichiamo con $\overline{H}$ la sua chiusura topologica in G. Per le dimostrazioni relative ai due risultati seguenti, rimandiamo a Bosch, *Algebra*, [8, § 4.2].

Lemma 2.3.4. Data L/K un'estensione di Galois e dato $H < \mathrm{Gal}(L/K)$, vale che

$$\overline{H} = \mathrm{Gal}(L/\operatorname{Fix}_H(L))$$

Teorema 2.3.5 (Corrispondenza di Galois - caso infinito)**.** Sia L/K un'estensione di Galois e sia $G = \mathrm{Gal}(L/K)$. Allora esistono due mappe

$$\begin{tikzcd} \{H < G \mid \overline{H} = H\} \arrow[rr, bend left, "\phi"] & & \{F \mid K \subset F \subset L\} \arrow[ll, bend left, "\psi"] \end{tikzcd}$$

che sono bigettive e l'una inversa dell'altra.

Un'antiequivalenza di categorie

Vogliamo ora estendere il funtore S visto nel caso finito ad un funtore tra la categoria $\mathfrak{A}$ delle K-algebre separabili e la categoria $\mathbb{G}$-$\mathfrak{Prof}$ degli spazi profiniti su cui $\mathbb{G}$ opera con continuità.

Sia $A \in \mathfrak{A}$: poniamo $S(A) = \mathrm{Hom}_K(A, \Omega_s) = \mathrm{Hom}_K(A, \Omega)$. Dati $x \in A$, $f \in S(A)$ e μ il polinomio minimo di x, si ha $\mu(f(x)) = 0$, da cui il polinomio minimo di $f(x)$ divide μ, e $f(x)$ separabile.
Notiamo che data B una sottoalgebra finita di A, l'insieme $\mathrm{Hom}_K(B, \Omega)$ è finito. Si ha $S(A) = \varprojlim \mathrm{Hom}_K(B, \Omega)$ al variare delle sottoalgebre finite di A. Tramite tale identificazione, $S(A)$ è uno spazio profinito.
L'azione di $\mathbb{G}$ su $S(A)$ definita da $g \cdot f = g \circ f$ è continua: infatti per ogni algebra étale B esiste un'estensione finita di Galois E che diagonalizza B (proposizione 2.2.6) per cui l'azione di $\mathbb{G}$ su $S(B)$ si fattorizza $\mathrm{Aut}_K(E)$ ed è dunque continua; in quanto limite proiettivo dei $\mathbb{G}$-insiemi $S(B)$ al variare di B tra le sottoalgebre finite di A, $S(A)$ è uno spazio profinito su cui $\mathbb{G}$ agisce con continuità, ossia $S(A) \in \mathbb{G}$-$\mathfrak{Prof}$.

Estendiamo ora il funtore S dalla categoria $\mathfrak{D}_L$ alla categoria $\mathfrak{A}$.

Teorema 2.3.6. Il funtore $S : \mathfrak{A} \to \mathbb{G}$-$\mathfrak{Prof}$ è un'antiequivalenza di categorie.

Dimostrazione. Siano $\mathfrak{E}_K$ la categoria delle K-algebre étale e, per ogni estensione E/K di Galois finita contenuta in Ω, $\mathfrak{D}_E$ la categoria delle K-algebre diagonalizzate da E. Denotiamo con G_E il gruppo di Galois $\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E)$. Dal teorema 2.2.7, il funtore $S_E : A \mapsto \mathrm{Hom}_K(A, E) = \mathrm{Hom}_K(A, \Omega)$ è un'antiequivalenza tra la categoria $\mathfrak{D}_E$ e la categoria G_E-$\mathfrak{FSet}$.
Per la proposizione 1.2.5, abbiamo che

$$\mathfrak{E}_K = \varinjlim_E \mathfrak{D}_E \ , \ \mathbb{G} = \varprojlim_E G_E \ , \ \mathbb{G}\text{-}\mathfrak{FSet} = \varinjlim_E G_E\text{-}\mathfrak{FSet}$$

I funtori S_E, passando al limite induttivo, definiscono un'antiequivalenza da $\mathfrak{E}_K$ a $\mathbb{G}$-$\mathfrak{FSet}$ ed è immediato verificare che tale antiequivalenza coincide con il funtore S. Notiamo infine che $\mathfrak{A}$ s'identifica alla categoria opposta dei pro-oggetti $\overrightarrow{\mathfrak{D}_E}$. D'altronde, per la proposizione 1.2.6, $\mathbb{G}$-$\mathfrak{Prof}$ $=$ $\mathbb{G}$-$\overleftarrow{\mathfrak{FSet}}$. Segue che S è un'antiequivalenza di categorie. $\square$

Enunciamo ora alcune proprietà e relazioni circa le algebra separabili su K. Siano A, B due K-algebre separabili, sia $f : A \to B$ omomorfismo tra esse e $f^* : S(B) \to S(A)$ mappa tra insiemi.

- f iniettivo (risp. surgettivo) $\iff$ f^* surgettivo (risp. iniettivo).
- A è un'estensione di campi di K $\iff$ $\mathbb{G}$ agisce transitivamente su $S(A)$. Più in generale, le orbite dell'azione di $\mathbb{G}$ su $S(A)$ sono in bigezione con gli ideali massimali di A.
- Possiamo associare ad ogni sottoestensione L di Ω_s lo stabilizzatore dell'inclusione canonica $i_L \in S(L)$. In tal modo, otteniamo una bigezione tra le sottoestensioni di Ω_s e i sottogruppi chiusi di $\mathbb{G}$. La bigezione inversa è data da $H \mapsto \mathrm{Fix}_H(\Omega_s)$.
- Siano L, L' sottoestensioni di Ω_s. Allora

$$L \cong L' \iff \exists g \in \mathbb{G} \ : \ \mathrm{Aut}_L(\Omega_s) = g(\mathrm{Aut}_{L'}(\Omega_s))g^{-1}$$

Riassumendo, sono definizioni equivalenti di estensione di Galois infinita le seguenti:

- L/K è separabile e $\forall g \in \mathbb{G}$ si ha $g(L) = L$;
- L è unione di sottoestensioni finite di Galois di Ω_s;
- $L \subset \Omega_s$ e $\mathrm{Aut}_L(\Omega_s) \lhd \mathbb{G}$.

Capitolo 3

Superfici di Riemann ed estensioni di campi

3.1 Rivestimenti ramificati su superfici di Riemann

In questa sezione presentiamo alcune proprietà delle superfici di Riemann e studiamo i rivestimenti ramificati finiti di una superficie topologica, arrivando ad un'equivalenza tra la categoria $\mathfrak{V}_B$ *dei rivestimenti ramificati analitici finiti su una superficie di Riemann compatta e connessa* B *e la categoria-limite* $\varinjlim_\Delta \mathfrak{FCov}_{B\setminus\Delta}$ *dei rivestimenti finiti su* $B \setminus \Delta$*, al variare di* Δ *tra gli insiemi di ramificazione su* B*.*

Diciamo che uno spazio topologico di Hausdorff X è una *superficie topologica* se ogni suo punto ammette un intorno omeomorfo ad un aperto di $\mathbb{R}^2$.
Diciamo che una superficie topologica X ammette un atlante di *carte complesse* se esiste una famiglia di omeomorfismi ϕ da un aperto $U \subset X$ in un aperto di $\mathbb{C}$, i cui domini ricoprono X. Diciamo che la carta ϕ è *centrata* in $x \in X$ se $x \in U$ e $\phi(x) = 0$. Date due carte (ϕ, U) e (ψ, V), un *cambio di carta* da ϕ a ψ è una mappa $\gamma : x \mapsto \psi(\phi^{-1}(x))$ che è omeomorfismo tra $\phi(U \cap V)$ e $\psi(U \cap V)$. Un atlante è detto $\mathbb{C}$-*analitico* se tutti i cambi di carta sono olomorfi.

Definizione. Una **superficie di Riemann** è una varietà $\mathbb{C}$-analitica di dimensione 1, ossia una superficie topologica munita di una struttura $\mathbb{C}$-analitica.

Siano X e Y superfici di Riemann.
Una funzione $f : X \to \mathbb{C}$ è *olomorfa* se per ogni carta complessa (ϕ, U) la mappa $z \mapsto f(\phi^{-1}(z))$ definita su $\phi(U)$ (detta *espressione* di f nella carta ϕ) è olomorfa.
Una mappa $f : X \to Y$ è *analitica* se, per ogni coppia di carte di X e di Y, le espressioni

di f in tali carte sono olomorfe.
Dato $D \subset X$ chiuso e discreto, una funzione $f : X \to \mathbb{C}$ è *meromorfa su X a poli in D* se $f : X \setminus D \to \mathbb{C}$ è olomorfa e $\forall d \in D$ esistono un intorno V di d e due funzioni g, h olomorfe su V tali che $h^{-1}(0) \subset \{d\}$ e $f|_{V \setminus \{d\}} = \frac{g}{h}$.

Notazioni.

$$\mathscr{O}(X) := \{f \text{ olomorfa su } X\}$$

$$\mathscr{M}(X, D) := \{f \text{ meromorfa su } X \text{ e a poli in } D\}$$

$$\mathscr{M}(X) := \varinjlim \mathscr{M}(X, D)$$

Vediamo ora una proposizione che introduce in concetto di ramificazione di una mappa analitica in un punto. Per la dimostrazione si fa riferimento a [9, § 6.1.4].

Proposizione 3.1.1. Siano X, Y due superfici di Riemann. Sia $f : X \to Y$ analitica. Siano $x_0 \in X$ e $y_0 = f(x_0) \in Y$. Supponiamo che f non sia costante in alcun intorno di x_0. Sia ψ una carta di Y centrata in y_0. Allora esiste una carta ϕ di X centrata in x_0 tale che l'espressione di f nelle carte ϕ e ψ sia della forma $z \mapsto z^d$ (ossia tale che $f(\phi^{-1}(x)) = \psi^{-1}(z^d)$).

Notiamo che il numero d non dipende dalla scelta delle carte. Tale numero è detto *indice di ramificazione* di f in x_0.

Proposizione 3.1.2. Siano X, X', Y, Y' superfici di Riemann, α, β, ϕ funzioni analitiche e ψ una mappa continua che fanno commutare il diagramma

$$\begin{tikzcd} X \arrow[r, "\psi"] \arrow[d, "\alpha"'] & X' \arrow[d, "\beta"] \\ Y \arrow[r, "\phi"'] & Y' \end{tikzcd}$$

Allora ψ è analitica.

La proposizione appena vista (per una dimostrazione, cf. [9, § 6.1.5]) ha come corollario il risultato seguente.

Corollario 3.1.3. Dato un atlante su una superficie di Riemann, i cambi di carte sono mappe analitiche.

Proposizione 3.1.4. Siano X, B superfici di Riemann con B connessa. Sia $\pi : X \to B$ analitica e propria. Allora sono equivalenti:

i) π non è costante su alcuna componente connessa di X;

ii) le fibre di π sono finite;

iii) $\forall X_i$ componente connessa di X, si ha $\pi(X_i) = B$;

iv) π è mappa aperta;

v) $\forall x \in X$ esistono una carta ϕ di X centrata in x e una carta ψ di B centrata in $\pi(x)$ tali che l'espressione di π nelle due carte sia $z \mapsto z^d$.

Parliamo ora di rivestimenti ramificati su superfici di Riemann.
Siano D_r il disco aperto di raggio r e centro 0 su $\mathbb{C}$, $D_r^\times = D_r \setminus \{0\}$ il disco puntato, $\forall k \in \mathbb{N}$ $D_q^\times$ il disco puntato di raggio $q = r^{1/k}$ e la mappa $f : D_q^\times \to D_r^\times$ tale che $z \mapsto z^k$.
Allora esiste un rivestimento connesso (normale) $(V^\times, p)$ di $D_r^\times$ di grado k, equivalente al rivestimento $(D_q^\times, f)$: infatti $\pi_1(D_r^\times) \cong \mathbb{Z}$, l'unico sottogruppo di indice k in $\mathbb{Z}$ è $k\mathbb{Z}$ (che è normale) e corrisponde proprio al rivestimento normale $(D_q^\times, f)$.
Dato $V^\times$ come sopra, consideriamo $V = V^\times \cup \{A\}$, l'estensione di p a $V \to D_r$ con $p(A) = 0$ e su V la topologia meno fine tale che $V \setminus \{A\}$ sia omeomorfo a $V^\times$ e $p : V \to D_r$ sia continua. Abbiamo che V è omeomorfo a D_q.

Proposizione 3.1.5. V ammette un'unica struttura analitica tale che p sia analitica. Tale struttura è indotta dalla struttura analitica di D_q tramite l'omeomorfismo $h : D_q \to V$.

Dimostrazione. Poichè $p \circ h = f$, la struttura analitica di V indotta da h soddisfa la condizione dell'enunciato. Per l'unicità, consideriamo un'altra struttura analitica su V. Furoi dallo 0, la mappa h è localmente rappresentabile come $h(z) = p^{-1}z^k$, dunque è analitica. Ma una mappa continua e analitica ovunque eccetto che in 0 è analitica anche in 0: quindi c'è un'unica struttura analitica su V tale che p sia analitica. $\square$

Definizione. Il passaggio dal rivestimento $(V^\times, p)$ di $D_r^\times$ al rivestimento (V, p) di D_r è detto operazione di **filling a hole**.

Grazie alla proposizione precedente, dopo aver "riempito un buco", lo spazio V ammette un'unica struttura di spazio analitico complesso per cui p è analitica.
Vogliamo ora estendere l'operazione di completamento a più "buchi".

Siano X una superficie di Riemann, M una varietà reale 2-dimensionale e $f : M \to X$ una mappa continua. Diciamo che f ha una *singolarità analitica* in $y \in M$ di molteplicità k se esistono un intorno puntato connesso $U^\times \subset X$ di $x = f(y)$ e una componente connessa dell'aperto $f^{-1}(U^\times)$ che sia intorno puntato $V^\times \subset M$ di y tali che $(V^\times, f)$ sia rivestimento di $U^\times$ di grado k. Moralmente, possiamo vedere y come la preimmagine di molteplicità k di x: in un intorno di un punto di singolarità analitica di molteplicità k, le fibre hanno cardinalità k.

Una mappa $f : M \to X$ è detta *rivestimento "branched"* se ha una singolarità analitica in ogni punto. I punti di molteplicità 1 sono detti *regolari*, quelli di molteplicità maggiore *singolari*. Inoltre:

- l'insieme dei punti regolari è aperto;
- la mappa è un omeomorfismo locale in un intorno di un punto regolare;
- l'insieme Δ dei punti singolari è un sottinsieme discreto di M;
- dato un rivestimento branched da una varietà reale 2-dimensionale M a una superficie di Riemann X, M ammette un'unica struttura di varietà complessa analitica tale che f sia analitica.

Costruiamo ora l'operazione di "filling holes".
Fissiamo una coordinata locale in $a \in X$ $(u(a) = 0)$ per cui abbiamo un'inversa da un intornino di a ad un intornino di $0 \in \mathbb{C}$. Sia $U^\times = u^{-1}(D_r^\times)$. Supponiamo che tra tutte le componenti connesse di $f^{-1}(U^\times)$ ce ne sia una $V^\times$ tale che $f|_{V^\times}$ sia un rivestimento di grado k. Allora possiamo applicare l'operazione di "filling a hole" a $V^\times$: taglio un intorno $V^\times$ da M e sostituisco il rivestimento $(V^\times, f)$ di $U^\times$ con la mappa $f : V \to U$ con l'operazione di "filling a hole", attaccando l'intorno V a $M \setminus V^\times$ con la mappa $f : V \to X$.

Definizione. Definisco dunque l'operazione di **filling holes** applicando le operazioni di "filling a hole" a tutti i buchi (nelle rispettive componenti connesse di $f^{-1}(U^\times)$) contemporaneamente.

Notiamo che tale operazione è ben definita poichè lo è su ogni componente connessa.

Siano X, M due superfici di Riemann, Δ sottinsieme discreto di X e $p : M \to X \setminus \Delta$ un rivestimento finito che è mappa analitica. Sia X connessa.
Per ogni $o \in \Delta$ consideriamo un intorno puntato $U^\times$ tale che $U^\times \cap \Delta = \{o\}$. Su tale intorno prendiamo un rivestimento $(V^\times, f)$ con $V^\times = f^{-1}(U^\times)$: allora $V^\times$ è unione di componenti connesse $V_i^\times$. Applichiamo l'operazione di "filling holes": su ogni $o \in \Delta$ attacchiamo un numero finito di punti, pari al numero delle componenti connesse di $V^\times$. Enunciamo ora un risultato classico di Analisi complessa.

Fatto. Sia $p : M \to X$ analitica tra varietà complesse tale che tutte le fibre hanno cardinalità k, con molteplicità. Allora la mappa è propria.

Lemma 3.1.6. Applicando l'operazione di "filling holes" a un rivestimento (M, p) di U di grado k, si ottiene una varietà complessa $\tilde{M}$ munita di una mappa propria analitica $\tilde{p} : \tilde{M} \to X$ di grado k.

Dimostrazione. Dalle costruzioni fatte fin ora sappiamo che $\tilde{M}$ è varietà complessa e $\tilde{p}$ è analitica. L' "essere propria" segue dalla proposizione precedente. □

Introduciamo ora il concetto di rivestimento ramificato. Fissiamo con X una superficie di Riemann connessa e con Δ un suo sottinsieme discreto.

Definizione. Siano $a \in X \backslash \Delta$. Un **rivestimento ramificato** su X con **ramificazione** su Δ è una terna $p : (M, b) \to (X, a)$, dove M è una varietà complessa e p una mappa analitica, i cui valori critici sono tutti contenuti in Δ.

Definiamo ora una nuova operazione, che vedremo essere l'inversa del "filling holes".

Definizione. Sia $p : M \to X$ un rivestimento ramificato connesso di X con ramificazione in Δ. Il passaggio da tale rivestimento ramificato al rivestimento (non ramificato) $p : M \setminus \tilde{\Delta} \to X \setminus \Delta$ con $\tilde{\Delta} = p^{-1}(\Delta)$ è detto operazione di *puntura di ramificazione* (o semplicemente **puntura**).

Anticipiamo un risultato che analizzeremo meglio più avanti.

Lemma 3.1.7. Le operaziondi di "filling holes" e di "puntura" sono l'una inversa dell'altra. Inoltre esse rappresentano un isomorfismo tra la categoria $\mathfrak{RCov}_{X,\Delta}$ dei rivestimenti ramificati di X con ramificazione in Δ e la categoria $\mathfrak{Cov}_{X \setminus \Delta}$ dei rivestimenti finiti di $X \setminus \Delta$.

Continuiamo a parlare di rivestimenti ramificati su superfici di Riemann, inquadrandoli però in un contesto categoriale con lo scopo di esplicitare alcune equivalenze di categorie.

Definizione. Sia B una superficie topologica. Un **rivestimento ramificato finito** di B è una superficie topologica X munita di una mappa continua propria $\pi : X \to B$ che verifica la proprietà:

> (*RR*) $\forall x \in X$ *esistono una carta complessa di* X *centrata in* x *e una carta complessa di* B *centrata in* $\pi(x)$ *tali che l'espressione di* π *in tali carte è della forma* $z \mapsto z^d$.

L'intero d della proprietà (*RR*) non dipende dalla scelta delle carte ed è detto *grado locale* o *indice di ramificazione* di X in x. L'insieme $\{x \in X \ : \ d > 1\}$ è un chiuso discreto di X: la sua proiezione Δ è un chiuso discreto di B, detto *insieme di ramificazione.* In tal caso, $(X \setminus \pi^{-1}(B \setminus \Delta), \pi)$ è un rivestimento finito di $B \setminus \Delta$. Se B è connesso e Δ è un chiuso discreto di B, allora $B \setminus \Delta$ è ancora connesso e i gradi locali del rivestimento in ogni punto sono tutti uguali. Allora si può parlare di *grado* di un rivestimento ramificato finito su una componente connessa di B.

Notiamo che i rivestimenti finiti di una superficie topologica sono rivestimenti ramificati finiti (il viceversa è falso). Inoltre, se X è un rivestimento ramificato finito di B, π è aperta e a fibre finite.

Definizione. Sia B una superfici di Riemann. Un **rivestimento ramificato analitico finito** di B è una superficie di Riemann X munita di una mappa analitica propria che soddisfa la proprietà (RR).

Notiamo che in questa definizione, per la proposizione 3.1.4, l'ipotesi che valga (RR) è equivalente all'ipotesi π *non è costante su alcuna componente connessa di* X.

Proposizione 3.1.8. Siano B una superficie topologica e (X, π) un suo rivestimento ramificato finito con insieme di ramificazione Δ. Dato $b \in B$, siano ϕ una carta di B centrata in b con dominio U, e V una componente connessa di $\pi^{-1}(U) \subset X$. Posto $U^* = U \setminus \{b\}$, supponiamo che $U^* \cap \Delta = \emptyset$. Allora $V(b) = V \cap \pi^{-1}(b)$ è costituita da un solo punto x, ed esiste una carta ψ di X centrata in x con dominio V tale che l'espressione di π nella carte ϕ e ψ è della forma $z \mapsto z^d$.

La proposizione precedente ci dice che preso un punto in b e un suo intorno U, ritroviamo la proprietà (RR) su ogni componente connessa di $\pi^{-1}(U)$. La dimostrazione della proposizione precedente (che non riportiamo) sfrutta il seguente risultato.

Lemma 3.1.9. Due rivestimenti connessi di U^* aventi lo stesso grado d sono isomorfi.

Dimostrazione. La carta ϕ centrata in b induce un omeomorfismo tra U^* e il disco puntato $D^* = D \setminus \{0\}$. Per ogni $\beta \in U^*$, il gruppo fondamentale topologico $\pi_1(U^*, \beta)$ è isomorfo a $\mathbb{Z}$. Per un risultato della teoria classica dei rivestimenti, le classi d'isomorfismo dei rivestimenti connessi di grado d di U^* sono in bigezione con le classi di coniugio dei sottogruppi di indice d in $\mathbb{Z}$. Essendo $\mathbb{Z}$ ciclico, sappiamo che c'è un unico sottogruppo per ogni indice, quindi c'è un'unica classe d'isomorfismo dei rivestimenti connessi di grado d di U^*. $\square$

Fissiamo B una superficie topologica. Mostriamo ora che da ogni rivestimento ramificato finito di B possiamo trovare un rivestimento ramificato *analitico* finito.

Proposizione 3.1.10. Sia (X, π) un rivestimento ramificato finito di B. Per ogni struttura $\mathbb{C}$-analitica su B, esiste una ed unica struttura $\mathbb{C}$-analitica su X tale che π sia analitica.

Dimostrazione. Sia $\Delta = (b_i)_I$ l'insieme di ramificazione di (X, π). Sia $(\phi_i)_I$ un atlante di B formato da carte centrate nei b_i di domini U_i tali che $(U_i \setminus \{b_i\}) \cap \Delta = \emptyset$.
Per ogni $i \in I$ consideriamo la famiglia $(V_{i,j})_{J_i}$ delle componenti connesse di $\pi^{-1}(U_i)$. Poniamo $J = \{(i,j) \ : \ j \in J_i\}$. Per la proposizione precedente, per ogni $(i,j) \in J$ esiste una carta $\psi_{i,j}$ di X per cui l'espressione di π nella carte $\psi_{i,j}$ e ϕ_i sia della forma $z \mapsto z^{d_{i,j}}$. Le $\psi_{i,j}$ formano un atlante di X e sappiamo che i cambi di carte sono analitici. Allora tale atlante definisce una struttura $\mathbb{C}$-analitica su X che rende π analitica.
L'unicità segue dalla proposizione 3.1.2. □

D'ora in avanti assumeremo B una superficie di Riemann compatta e connessa. Consideriamo la categoria $\mathfrak{V}_B$ dei rivestimenti ramificati analitici finiti su B con morfismi le surgezioni analitiche su B, e la categoria $\mathfrak{RCov}_B$ dei rivestimenti ramificati finiti (topologici, senza struttura analitica) con morfismi le surgezioni continue su B.

Corollario 3.1.11. Il funtore d'oblio identifica le categorie $\mathfrak{V}_B$ e $\mathfrak{RCov}_B$.

Dimostrazione. L'identificazione tra oggetti è data dalla proposizione precedente, mentre quella tra morfismi segue dalla proposizione 3.1.2. □

Torniamo ora a considerare una superficie topologica B (senza alcuna struttura analitica sopra). Sia Δ un chiuso discreto in B. Indichiamo con $\mathfrak{RCov}_{B,\Delta}$ la categoria dei rivestimenti ramificati finiti su B con ramificazione contenuta in Δ, e con $\mathfrak{FCov}_{B\setminus\Delta}$ la categoria dei rivestimenti finiti di $B \setminus \Delta$.
Un risultato utile per raggiungere lo scopo di questa sezione è la seguente equivalenza di categorie, già accennata nel lemma 3.1.7. Per una dimostrazione, si rimanda a [9, § 6.1.11].

Proposizione 3.1.12. Il funtore $\rho : X \mapsto X \cap \pi^{-1}(B \setminus \Delta)$ è un'equivalenza tra le categorie $\mathfrak{RCov}_{B,\Delta}$ e $\mathfrak{FCov}_{B\setminus\Delta}$.

Notiamo che il funtore ρ rappresenta l'operazione di *puntura*, mentre il suo funtore quasi-inverso rappresenta l'operazione di *filling holes*.

Siamo dunque pronti per enunciare e dimostrare il risultato finale di questa sezione.
Sia B una superficie di Riemann compatta e connessa. Indichiamo con I l'insieme ordinato (per inclusione) dei chiusi discreti di B. Consideriamo il funtore ω che ad ogni $X \in \mathfrak{V}_B$ associa il rivestimento topologico finito $X \cap \pi^{-1}(B \setminus \Delta)$ (privo di struttura analitica), con Δ l'insieme di ramificazione di (X, π).

Teorema 3.1.13. Il funtore $\omega : \mathfrak{V}_B \to \varinjlim_I \mathfrak{FCov}_{B\setminus\Delta}$ è un'equivalenza di categorie.

Dimostrazione. Dall'ultimo corollario visto, sappiamo che $\mathfrak{V}_B$ s'identifica tramite il funtore di oblio alla categoria $\mathfrak{RCov}_B$. Notiamo che

$$\mathfrak{RCov}_B = \bigcup_{\Delta} \mathfrak{RCov}_{B,\Delta} = \varinjlim \mathfrak{RCov}_{B,\Delta}$$

Per la proposizione precedente, sappiamo che le categorie $\mathfrak{RCov}_{B,\Delta}$ e $\mathfrak{FCov}_{B\setminus\Delta}$ sono equivalenti. Passando al limite induttivo, abbiamo la tesi. □

3.2 Equivalenza tra rivestimenti ramificati e algebre étale

In questa sezione spostiamo la nostra attenzione sul campo delle funzioni meromorfe su una superficie di Riemann, e sulle algebre che sono étale su tale campo. Il nostro obiettivo è giungere ad un'antiequivalenza tra la categoria $\mathfrak{V}_B$ dei rivestimenti ramificati analitici finiti su una superficie di Riemann compatta e connessa B e la categoria $\mathfrak{E}$ delle algebre étale sul campo $K = \mathscr{M}(B)$.

Per i nostri scopi daremo per buono il seguente risultato, che richiederebbe una trattazione abbastanza articolata. Per una dimostrazione, è possibile consultare *Algebraic curves and Riemann surfaces* di R. Miranda ([5, Cap VI]).

Teorema 3.2.1 (di separazione)**.** Siano X una superficie di Riemann e $a, b \in X$ due punti distinti. Allora esiste una funzione meromorfa $f : X \to \mathbb{C}$ definita in a e b tale che $f(a) \neq f(b)$.

Corollario 3.2.2. Siano X una superficie di Riemann e $a_1, \dots, a_d \in X$ distinti. Allora esiste una funzione meromorfa f su X definita in ciascun a_i e tale che i valori $f(a_i)$ sono due a due distinti.

Vediamo ora un criterio analitico di meromorfia su superfici di Riemann legato al concetto di *singolarità algebrica*.

Proposizione 3.2.3. Siano X una superficie di Riemann, D un suo chiuso discreto e $f : X \setminus D \to \mathbb{C}$ una funzione olomorfa. Siano $a \in X$ e ϕ una carta di X centrata in a di dominio U. Allora f è meromorfa in a se e solo se esistono un intorno aperto $U' \subset U$ di a e delle costanti $c, k \in \mathbb{R}$ tali che

$$\forall x \in U' \setminus \{a\} \ , \quad |f(x)| \leq c \cdot |\phi(x)|^{-k}$$

Dimostrazione. Se la condizione è soddisfatta, allora la mappa $x \mapsto (\phi(x))^k f(x)$ è olomorfa su $U \setminus \{a\}$, limitata nell'intorno di a in cui si prolunga olomorficamente su U.

Se f è meromorfa su a, in un intorno di a f è della forma $\frac{g(x)}{\phi(x)^k u(x)}$ con u olomorfa e $u(a) \neq 0$. Allora u è invertibile in un intorno di a e $\frac{g}{u}$ è limitata su un intorno U' di a da una costante c, da cui si ha la tesi per ogni $u \in U' \setminus \{a\}$. $\square$

Fissiamo ora B una superficie di Riemann connessa e compatta.
Il nostro intento è passare dalla categoria $\mathfrak{V}_B$ dei rivestimenti ramificati analitici finiti di B alla categoria $\mathfrak{E}_B$ delle algebre étale sul campo $K = \mathscr{M}(B)$ e viceversa.

Data X una superficie di Riemann, ricordiamo che, in generale, l'insieme delle funzioni meromorfe $\mathscr{M}(X)$ è una $\mathbb{C}$-algebra. Inoltre, se X è connessa, $\mathscr{M}(X)$ è un campo. Date due superfici di Riemann X, Y e una funzione analitica $f : X \to Y$ non costante sulle componenti connesse di X, definiamo l'omomorfismo di algebre $f^* : \mathscr{M}(Y) \to \mathscr{M}(X)$ dato da $f^*(h) = h \circ f$. Se $D \subset Y$ è l'insieme dei poli di h, allora $f^*(h)$ è definita su $X \setminus f^{-1}(D)$. Inoltre, vale che $(g \circ f)^* = f^* \circ g^*$.
Per quanto detto, $\mathscr{M}$ rispetta le proprietà di funtorialità. Vediamo ora che effettivamente $\mathscr{M}$ è un funtore da $\mathfrak{V}_B$ e $\mathfrak{E}_B$.

Teorema 3.2.4. Sia (X, π) un rivestimento ramificato analitico di B di grado d. Allora $\mathscr{M}(X)$ è un'algebra étale su $\mathscr{M}(B)$ di grado d.

Dimostrazione.

- Sia $f \in \mathscr{M}(X)$. Vediamo che f è algebrica su $\mathscr{M}(B)$ di grado $\leq d$. Cerchiamo quindi un polinomio $P \in \mathscr{M}(B)[Z]$ tale che $P(f) = 0$.
  Denotiamo con $\Delta_r \subset B$ l'insieme di ramificazione di X su B tramite π, con $\Delta_p \subset B$ la proiezione dell'insieme dei poli di f e poniamo $\Delta = \Delta_r \cup \Delta_p$. Sia dunque $b \in B \setminus \Delta$ e sia $\pi^{-1}(b) = \{x_1, \dots, x_d\}$: siano $a_1(b), \dots, a_d(b)$ i valori delle funzioni simmetriche elementari di grado d valutate negli $f(x_i)$. Ragionando sugli aperti banalizzanti del rivestimento e usando il criterio di meromorfia 3.2.3, per ogni i si ha che $a_i \in \mathscr{M}(B)$. Consideriamo dunque il polinomio

  $$P(Z) = Z^d + \sum_i (-1)^i a_i Z^{d-i} \in \mathscr{M}(B)[Z]$$

  e dimostriamo che $P(f) = 0$ in $\mathscr{M}(X)$. Sia $x \in \pi^{-1}(b)$. Il polinomio $P_b(Z) = Z^d + \sum_i (-1)^i a_i(b) Z^{d-i}$ ha per radici $f(x_1), \dots, f(x_d)$ e in particolare

  $$f(x)^d + \sum_{i=1}^{d} (-1)^i a_i(b) f(x)^{d-i} = 0$$

  ossia $P(f)(x) = 0$. Poichè ciò vale per ogni $x \in \pi^{-1}(B \setminus \Delta)$, si ha $P(f) = 0$.

- Vediamo che $\mathscr{M}(X)$ è étale su $\mathscr{M}(B)$ di grado $\leq d$.
  Possiamo supporre X connesso. In tal caso, $\mathscr{M}(X)$ è un'estensione di $\mathscr{M}(B)$ che è unione filtrante di estensioni E_λ di tipo finito di $\mathscr{M}(B)$. Ciascuna E_λ è finitamente generata e algebrica, dunque è finita. Poichè $char\mathscr{M}(B) = 0$, segue che E_λ è separabile (dunque étale). Per il teorema dell'elemento primitivo (2.1.5), E_λ è un'estensione semplice di $\mathscr{M}(B)$ e quindi di grado $\leq d$. Segue che $\mathscr{M}(X)$ è di grado $\leq d$ su $\mathscr{M}(B)$.

- Vediamo che $\mathscr{M}(X)$ è di grado $\geq d$.
  Sia $b_0 \in B \setminus \Delta_r$, con Δ_r definito nel primo punto della dimostrazione, tale che $\pi^{-1}(b_0) = \{x_1, \ldots, x_d\}$ e sia $f \in \mathscr{M}(X)$ definita sugli x_i prendendo in questi punti valori due a due distinti (esiste per 3.2.2). Mostriamo che il polinomio minimo di f su $\mathscr{M}(B)$ è di grado $\geq d$.
  Sia $P = \sum_{i=0}^{k} c_i Z^i \in \mathscr{M}(B)[Z]$ tale che $P(f) = 0$: allora per ogni $x \in X$ e $b = \pi(x)$ per i quali $f(x), c_i(b)$ sono definiti, si ha $\sum_{i=0}^{k} c_i(b)(f(x))^i = 0$. Vediamo che $k \geq d$: se b è sufficientemente vicino a b_0 e non è polo di alcun c_i, allora il polinomio $P_b = \sum c_i(b)Z^i \in \mathbb{C}[Z]$ ha almeno d radici distinte (per come è stata scelta f tramite il corollario 3.2.2) ed esse sono proprio i valori $f(x_1), \ldots, f(x_d)$. In particolare, il polinomio minimo di f ha grado $\geq d$, da cui $[\mathscr{M}(X) : \mathscr{M}(B)] \geq d$.

$\square$

Osservazione. Dati (X, π) rivestimento ramificato analitico finito di B con ramificazione su $\Delta \subset B$ e $b \in B \setminus \Delta$, consideriamo f una funzione definita sui punti di $\pi^{-1}(b)$ e ne prendiamo i valori due a due distinti in questi punti. Dalla dimostrazione segue che f genera $\mathscr{M}(X)$ come $\mathscr{M}(B)$-algebra.

Vogliamo dunque mostrare che il funtore $\mathscr{M} : \mathfrak{V}_B \to \mathfrak{E}_B$ fornisce proprio l'antiequivalenza di categorie cercata. Per raggiungere tale scopo, procederemo per i seguenti steps:

- ◇ Data un'algebra E étale su $K = \mathscr{M}(B)$ e un suo elemento primitivo ζ, *costruiamo* un rivestimento finito $\mathscr{S}(E, \zeta)$ di $B \setminus \Delta_{E,\zeta}$, dove $\Delta_{E,\zeta}$ è un chiuso discreto legato a ζ.

- ◇ Dato un omomorfismo di algebre étale $\alpha : E \to F$, definiamo una mappa continua $\alpha^* : \mathscr{S}(F, \theta) \to \mathscr{S}(E, \zeta)$ e verifichiamo le proprietà funtoriali di $\alpha \mapsto \alpha^*$. Grazie ai due passi precedenti, possiamo parlare del funtore $\mathscr{S} : \mathfrak{E}_B \to \varinjlim \mathfrak{FCov}_{B\setminus\Delta}$.

- ◇ Passiamo dalla categoria $\varinjlim \mathfrak{FCov}_{B\setminus\Delta}$ alla categoria $\mathfrak{V}_B$ tramite l'operazione di *filling holes* ottenendo il funtore $\hat{\mathscr{S}} : \mathfrak{E}_B \to \mathfrak{V}_B$, candidato ad essere il funtore quasi-inverso di $\mathscr{M}$.

- ◇ Mostriamo che il funtore $\mathscr{M}$ è essenzialmente surgettivo.
- ◇ Mostriamo che il funtore $\mathscr{M}$ è pienamente fedele.

Sia E un'algebra étale su $\mathscr{M}(B)$ e sia $\zeta \in E$ un suo elemento primitivo. Consideriamo il suo polinomio minimo $P(Z) = Z^d + a_1 Z^{d-1} + \cdots + a_d \in \mathscr{M}(B)[Z]$. Denotiamo con $\Delta_{E,\zeta}$ l'insieme dei poli dei coefficienti di P unito all'insieme degli zeri del discriminante $\operatorname{disc}(P)$ di P. Notiamo che per ogni $b \in B \setminus \Delta_{E,\zeta}$, il polinomio $P_b(Z) = Z^d + a_1(b) Z^{d-1} + \cdots + a_d(b)$ ha esattamente d radici distinte. Inoltre, $\Delta_{E,\zeta}$ è un sottinsieme chiuso discreto (quindi finito poichè chiuso discreto in un compatto) di B.
Definiamo quindi il sottospazio di $(B \setminus \Delta_{E,\zeta}) \times \mathbb{C}$

$$\mathscr{S}(E,\zeta) = \{(b,z) \in (B \setminus \Delta_{E,\zeta}) \times \mathbb{C} \ : \ P_b(z) = 0\}$$

e notiamo che la proiezione sulla prima componente $\pi : \mathscr{S}(E,\zeta) \to B \setminus \Delta_{E,\zeta}$ è un rivestimento finito di grado di d.

Vogliamo ora, dato $\alpha : E \to F$ omomorfismo di $\mathscr{M}(B)$-algebre étale e dati ζ, θ elementi primitivi (risp.) di E ed F, definire una mappa continua

$$\alpha^* : \mathscr{S}(F,\theta) \to \mathscr{S}(E,\zeta)$$

nella categoria $\varinjlim \mathfrak{FCov}_{B \setminus \Delta}$. Siano P, Q i polinomi minimi (risp.) di ζ e θ su $\mathscr{M}(B)$. Poichè θ genera F come $\mathscr{M}(B)$-algebra, l'elemento $\alpha(\zeta) \in F$ è della forma $R(\theta)$ con $R \in \mathscr{M}(B)[Z]$. Indichiamo con $\Delta'_R \subset B$ l'insieme dei poli dei coefficienti di R e definiamo la mappa $\tilde{R} : (B \setminus \Delta'_R) \times \mathbb{C} \to (B \setminus \Delta'_R) \times \mathbb{C}$ data da $(b,z) \mapsto (b, R_b(z))$.

Lemma 3.2.5. L'applicazione $\tilde{R}$ induce un'applicazione

$$\alpha^* : \mathscr{S}(F,\theta) \cap \pi^{-1}(B \setminus \Delta'_R) \to \mathscr{S}(E,\zeta)$$

che non dipende dalla scelta di R.

Dimostrazione. Poichè si ha $P(R(\theta)) = P(\alpha(\zeta)) = \alpha(P(\zeta)) = 0 \in F$, abbiamo che $P \circ R$ è della forma $Q \cdot V$ con $V \in \mathscr{M}(B)[Z]$, ossia abbiamo $P_b(R_b(z)) = Q_b(z) V_b(z)$ per $z \in \mathbb{C}$ e $b \in B$ tale che i coefficienti di P, Q, R, V siano definiti. Se $(b,z) \in \mathscr{S}(F,\theta)$, allora $Q_b(z) = 0$, da cui $P_b(R_b(z)) = 0$ e $\tilde{R}_b(z) = (b, R_b(z)) \in \mathscr{S}(E,\zeta)$.
Vediamo che tale applicazione non dipende da R. Sia $R_1 \in \mathscr{M}(B)[Z]$ un altro polinomio tale che $\alpha(\zeta) = R_1(\theta)$. Il polinomio $R - R_1$ si annulla in θ, dunque è della forma $Q \cdot W$ con $W \in \mathscr{M}(B)[Z]$. Ma allora $R_b(z) = R_{1b}(z) \iff Q_b(z) = 0$, da cui $\tilde{R} = \tilde{R}_1$ in $\mathscr{S}(F,\theta)$. □

Vediamo ora la funtorialità di $\alpha \mapsto \alpha^*$.
Date E, F, G tre algebre étale su $\mathscr{M}(B)$ con elementi primitivi (risp.) ζ, θ, λ, consideriamo $\alpha : E \to F$ e $\beta : F \to G$ omomorfismi di algebre. Allora $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$: infatti, dati $R_1, R_2 \in \mathscr{M}(B)[Z]$ tali che $\alpha(\zeta) = R_1(\theta)$ e $\beta(\theta) = R_2(\lambda)$, si ha $\beta \circ \alpha(\zeta) = R_1(R_2(\lambda))$ e possiamo scegliere $R_3 = R_1 \circ R_2$ tale che $\beta \circ \alpha(\zeta) = R_3(\lambda)$; quindi $(\beta \circ \alpha)^*$ è indotto da $\tilde{R_3} = \tilde{R_1} \circ \tilde{R_2}$, da cui $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$.
Concludiamo dunque che $\mathscr{S}$ è un funtore da $\mathfrak{E}_B$ a $\varinjlim \mathfrak{FCov}_{B \setminus \Delta}$.

Sia $(X, \pi) \in \mathfrak{V}_B$ e sia $\Delta_X \subset B$ il suo insieme di ramificazione. Data $f \in \mathscr{M}(X)$, denotiamo con $\Delta'_f \subset B$ la proiezione tramite π dell'insieme dei poli di f.
Supponiamo che esista $b \in B \setminus \Delta_X$ tale che f sia definita su tutto $\pi^{-1}(b)$ e supponiamo che f in $\pi^{-1}(b)$ assuma valori a due a due distinti. Allora dall'osservazione al teorema 3.2.4 segue che f genera $\mathscr{M}(X)$ come $\mathscr{M}(B)$-algebra étale. Possiamo dunque considerare il rivestimento

$$\mathscr{S}(\mathscr{M}(X), f) \to B \setminus \Delta_f$$

e poniamo $\Delta = \Delta_X \cup \Delta_f \cup \Delta'_f$ e $\Delta^{-1} = \pi^{-1}(\Delta)$.

Proposizione 3.2.6. La mappa $(\pi, f) : X \setminus \Delta^{-1} \to (B \setminus \Delta) \times \mathbb{C}$ induce un isomorfismo di rivestimenti tra $X \setminus \Delta^{-1}$ e $\mathscr{S}(\mathscr{M}(X), f) \setminus \Delta^{-1}$.

Dimostrazione. Sia P il polinomio minimo di f in $\mathscr{M}(X)$. Per ogni $x \in X$ su cui f sia definita e i coefficienti di P siano definiti in $b = \pi(x)$, si ha $P_b(f(z)) = 0$. Segue che l'immagine di (π, f) è contenuta in $\mathscr{S}(\mathscr{M}(X), f)$ e commuta con le proiezioni, quindi è un morfismo di rivestimenti.
Se $b \in \Delta$ (è possibile vedere che tale caso non si verifica mai), consideriamo $b' \in B \setminus \Delta$ in un intorno di b in modo che b' soddisfi ancora le ipotesi fatte su b. Allora il morfismo di rivestimenti (π, f) è bigettivo sulla fibra di b', e ne segue che è un isomorfismo. $\square$

Vogliamo ora, partendo da un'algebra étale, ottenere un isomorfismo di algebre, che ci permetterà di provare la surgettività essenziale del funtore $\mathscr{M} : X \mapsto \mathscr{M}(X)$ che ad ogni superficie di Riemann associa la sua algebra delle funzioni meromorfe.
Sia $E \in \mathfrak{E}_B$ e sia $\zeta \in E$ un suo elemento primitivo. Consideriamo il rivestimento $\mathscr{S}(E, \zeta)$ di $B \setminus \Delta_{E,\zeta}$. Applicando l'operazione di *filling holes* (ossia tramite l'equivalenza tra $\mathfrak{V}_B$ e $\varinjlim \mathfrak{FCov}_{B \setminus \Delta}$ data dal funtore ω), otteniamo un rivestimento ramificato analitico $\hat{\mathscr{S}}(E, \zeta)$ di B tale che $\hat{\mathscr{S}}(E, \zeta) \setminus \Delta_{E,\zeta} = \mathscr{S}(E, \zeta)$.
Denotiamo con Z la proiezione sulla seconda componente $\hat{\mathscr{S}}(E, \zeta) \to \mathbb{C}$.
Enunciamo ora un semplice risultato, utile per la proposizione successiva.

Fatto. Sia $P = Z^d + a_1 Z^{d-1} + \cdots + a_d \in \mathbb{C}[Z]$ e sia z una sua radice. Allora

$$|z| \leq \sup(1, |a_1| + \cdots + |a_d|)$$

Proposizione 3.2.7 (Surgettività essenziale di $\mathscr{M}$).

i) La mappa Z è meromorfa su $\hat{\mathscr{S}}(E, \zeta)$.

ii) Esiste uno ed unico isomorfismo di algebre $\phi : E \to \mathscr{M}(\hat{\mathscr{S}}(E, \zeta))$ tale che $\phi(\zeta) = Z$.

Dimostrazione.

i) Ovviamente Z è olomorfa su $B \setminus \Delta$. Siano $b \in \Delta$ e $x \in \pi^{-1}(b) \subset X = \hat{\mathscr{S}}(E, \zeta)$. Siano ϕ una carta di B centrata in b e ψ una carta di X centrata in x tali che π rispetto alle due carte è della forma $z \mapsto z^r$. Sia $P = Z^d + a_1 Z^{d-1} + \cdots + a_d$ il polinomio minimo di ζ con $a_i \in \mathscr{M}(B)$: siano $\tilde{a}_i$ le rispettive espressioni rispetto la carta ϕ. Per x' in un intorno di x, il valore $Z(x')$ è radice del polinomio $P_{b'} = Z^d + a_1(b') Z^{d-1} + \cdots + a_d(b')$ con $b' = \pi(x')$: per il fatto enunciato prima, si ha la maggiorazione

$$|Z(x')| \leq \sup(1, \sum_i |a_i(b')|)$$

Si ha $a_i(b') = \tilde{a}_i(\phi(b)) = \tilde{a}_i(\psi(x')^r)$. Poichè le a_i sono meromorfe, esse ammettono una maggiorazione del tipo $|a_i(y)| \leq c|\phi(y)|^{-k}$, dunque lo stesso vale per Z. Segue che Z è meromorfa.

ii) Sia P il polinomio minimo di ζ su $\mathscr{M}(B)$: $\forall (b, z) \in \mathscr{S}(E, \zeta)$ vale $P_b(z) = 0$, ossia $P(Z) = 0$ in $\mathscr{M}(X)$. Vediamo che P è il polinomio minimo di Z in $\mathscr{M}(X)$. Sia $Q \in \mathscr{M}(B)[Z]$ tale che $Q(Z) = 0$: mostriamo che $P \mid Q$. A meno di dividere Q per P, possiamo supporre che $\deg Q \lneq d = \deg P$. Allora $\forall b \in B \setminus \Delta$ su cui i coefficienti di Q sono definiti, si ha $\pi^{-1}(b) = \{(b, z) \ : \ P_b(z) = 0\}$, dunque le radici di P_b sono radici di Q_b e, poichè ce ne sono d distinte, si $Q_b = 0$, da cui $Q = 0$ e P è il polinomio minimo di Z in $\mathscr{M}(X)$.
Esiste dunque uno ed unico omomorfismo di $\mathscr{M}(B)$-algebre $\phi : E \to \mathscr{M}(X)$ tale che $\phi(\zeta) = Z$, e tale ϕ è iniettivo. Per ipotesi E è un'algebra di grado d su $\mathscr{M}(B)$ e X è un rivestimento ramificato di grado d, da cui $\mathscr{M}(X)$ è un'algebra di grado d per il teorema 3.2.4. Per questioni di grado, ϕ è un isomorfismo.

□

Resta ora da verificare che il funtore $\mathscr{M}$ è pienamente fedele.

Proposizione 3.2.8 (Fedeltà piena)**.** Siano $X, Y \in \mathfrak{V}_B$ e sia $u : \mathscr{M}(X) \to \mathscr{M}(Y)$ un omomorfismo di $\mathscr{M}(B)$-algebre. Allora esiste un morfismo $h : Y \to X$ tale che $h^* = u$.

Dimostrazione. Siano f, g due elementi primitivi di (risp.) $\mathscr{M}(X)$ e $\mathscr{M}(Y)$ tali che

$$X \setminus \Delta_1^{-1} \cong \mathscr{S}(\mathscr{M}(X), f) \setminus \Delta_1^{-1} \quad , \quad Y \setminus \Delta_2^{-1} \cong \mathscr{S}(\mathscr{M}(Y), g) \setminus \Delta_2^{-1}$$

con i Δ_i dati dalla proposizione 3.2.6. I due isomorfismi si prolungano agli isomorfismi

$$\tilde{f} : X \to \hat{\mathscr{S}}(\mathscr{M}(X), f) \quad , \quad \tilde{g} : Y \to \hat{\mathscr{S}}(\mathscr{M}(Y), g)$$

Analogamente, il morfismo $u^* : \mathscr{S}(\mathscr{M}(Y), g) \to \mathscr{S}(\mathscr{M}(X), f)$ si prolunga tramite il funtore ω ad un morfismo $u^* : \hat{\mathscr{S}}(\mathscr{M}(Y), g) \to \hat{\mathscr{S}}(\mathscr{M}(X), f)$. Definiamo $h : Y \to X$ tramite la commutatività del diagramma

$$\begin{tikzcd}
Y \arrow[r, "h"] \arrow[d, "\tilde{g}"'] & X \arrow[d, "\tilde{f}"] \\
\hat{\mathscr{S}}(\mathscr{M}(Y), g) \arrow[r, "u^*"'] & \hat{\mathscr{S}}(\mathscr{M}(X), f)
\end{tikzcd}$$

Resta da verificare che $h^* = u$. Poichè f genera $\mathscr{M}(X)$, basta mostrare che $u(f) = h^*(f) = f \circ h : Y\mathbb{C}$. Abbiamo che $f \circ h = Z \circ \tilde{f} \circ h = Z \circ u^* \circ \tilde{g}$. Per ogni $y \in \pi_Y^{-1}(b)$, si ha

$$u^*(\tilde{g}(y)) = u^*(b, g(y)) = \tilde{R}(b, g(y)) = (b, R(b, g(y)))$$

con $R \in \mathscr{M}(B)$ tale che $u(f) = R(g)$. Quindi abbiamo $Z \circ u^* \circ \tilde{g} = R(g) = u(f)$, da cui $h^* = u$.
Per l'unicità, notiamo che, se anche $h_1^* = u$, si ha $h_1^*(f) = h^*(f)$, ossia $f \circ h_1 = f \circ h$, da cui $\tilde{f} \circ h_1 = \tilde{f} \circ h$ e, poichè $\tilde{f}$ è isomorfismo, si ha $h_1 = h$. □

Dalle ultime due proposizioni segue il risultato centrale di questa trattazione. Siano $\mathfrak{V}_B$ la categoria dei rivestimenti ramificati analitici finiti di una superficie di Riemann compatta e connessa B, $\mathfrak{E}_B$ la categoria delle algebre étale su $\mathscr{M}(B)$ e $\mathscr{M} : X \mapsto \mathscr{M}(X)$ il funtore che ad ogni superficie di Riemann associa la sua algebra delle funzioni meromorfe.

Teorema 3.2.9. Sia B una superficie di Riemann connessa e compatta. Il funtore $\mathscr{M} : \mathfrak{V}_B \to \mathfrak{E}_B$ è un'antiequivalenza di categorie.

Corollario 3.2.10. Siano $X, Y \in \mathfrak{V}_B$ e sia $\Delta \subset B$ un insieme finito tale che X e Y non abbiano ramificazioni su $B \setminus \Delta$. Allora $\mathrm{Hom}_{\mathfrak{E}_B}(\mathscr{M}(X), \mathscr{M}(Y))$ s'identifica a $\mathrm{Hom}_{\mathfrak{FCov}_{B\setminus\Delta}}(Y \setminus \Delta^{-1}, X \setminus \Delta^{-1})$.

Riassumendo, scegliendo per ogni $E \in \mathfrak{E}_B$ un elemento primitivo, possiamo definire un funtore $\mathscr{S} : \mathfrak{E}_B \to \varinjlim \mathfrak{FCov}_{B\setminus\Delta}$ e otteniamo il diagramman commutativo

$$\begin{tikzcd} \mathfrak{V}_B \arrow[r, "\mathscr{M}"] \arrow[d, "\omega"'] & \mathfrak{E}_B \arrow[dl, "\mathscr{S}"] \\ \varinjlim \mathfrak{FCov}_{B\setminus\Delta} & \end{tikzcd}$$

Notiamo che in questo diagramma ω è un'equivalenza, mentre $\mathscr{M}$ e $\mathscr{S}$ sono antiequivalenze.

Enunciamo alcune proprietà derivanti da questa equivalenza di categorie. Siano $X, Y \in \mathfrak{V}_B$.

- Il grado di $\mathscr{M}(X)$ come algebra étale su $\mathscr{M}(B)$ è uguale al grado di X su B.

- $\mathscr{M}(X)$ è un'estensione di campi di $\mathscr{M}(B) \iff X$ è connesso.
  Esiste una corrispondenza biunivoca tra le componenti connesse di X e gli ideali massimali di $\mathscr{M}(X)$.

- Sia $f : X \to Y$ un morfismo e sia $f^* : \mathscr{M}(Y) \to \mathscr{M}(X)$. Allora f è iniettivo (risp. surgettivo) $\iff$ f^* è surgettivo (risp. iniettivo).

- $\mathscr{M}(X \sqcup Y) = \mathscr{M}(X) \times \mathscr{M}(Y)$.
  Siano $X \times_B Y$ prodotto fibrato, $\Delta = \Delta_Y \cup \Delta_Y \subset B$ e $Z \in \mathfrak{V}_B$ tale che $Z \setminus \Delta^{-1} = (X \times_B Y) \setminus \Delta^{-1}$. Allora $\mathscr{M}(Z) = \mathscr{M}(X) \otimes_{\mathscr{M}(B)} \mathscr{M}(Y)$.

Vediamo ora un corollario del teorema 3.2.9 che si collega alla teoria di Galois per estensioni di campi. Ricordiamo che se il rivestimento X di B è connesso, allora $\mathscr{M}(X)/\mathscr{M}(B)$ è un'estensione di campi. Inoltre, definiamo *gruppo opposto* ad un dato gruppo come l'analogo della categoria opposta ad una data categoria (cf. Cap I).

Teorema 3.2.11. Sia $X \in \mathfrak{V}_B$ connesso e sia $\Delta \subset B$ un insieme finito contenente l'insieme di ramificazione di X. Allora $\mathscr{M}(X)/\mathscr{M}(B)$ è un'estensione di Galois *se e solo se* $X \setminus \Delta^{-1}$ è un rivestimento galoisiano di $B \setminus \Delta$.
In tal caso, il gruppo di Galois algebrico $\mathrm{Gal}(\mathscr{M}(X)/\mathscr{M}(B))$ s'identifica al gruppo opposto al gruppo di Galois topologico $\mathrm{Aut}_{B\setminus\Delta}(X \setminus \Delta^{-1})$. In particolare, tali gruppi sono isomorfi.

Notiamo che l'identificazione dei due gruppi di Galois segue dalla fedeltà piena del funtore $\mathscr{M}$.

Terminiamo la sezione definendo l'insieme di ramificazione di un'algebra étale su $\mathscr{M}(B)$. Sia E una $\mathscr{M}(B)$-algebra étale: per il teorema 3.2.9, sappiamo che E è isomorfa ad un'algebra della forma $\mathscr{M}(X)$ con X rivestimento ramificato analitico finito di B. Denotiamo con $\Delta_E \subset B$ l'insieme di ramificazione di X: diciamo che Δ_E è l'*insieme di ramificazione dell'algebra* E.
Vediamo alcune proprietà di questo insieme in termini di algebre:

- Se F è una sottoalgebra o un quoziente di E, allora $\Delta_F \subset \Delta_E$.

- Se E, F sono due algebre étale su $\mathscr{M}(B)$, si ha

$$\Delta_{E\times F} = \Delta_E \cup \Delta_F \quad , \quad \Delta_{E\otimes F} \subset \Delta_E \cup \Delta_F$$

  e la seconda relazione è un'uguaglianza se $E, F \neq (0)$ (infatti in tal caso E, F sono sottoalgebre di $E \otimes F$).

- Se F, G sono sottoalgebre di un'algebra étale E su $\mathscr{M}(B)$, si ha $\Delta_{F.G} = \Delta_F \cup \Delta_G$.

Con la seguente proposizione esplicitiamo Δ_E in relazione agli insiemi $\Delta_{E,\zeta}$ con ζ un elemento primitivo di E. Per una dimostrazione rimandiamo a [9, § 6.2.12].

Proposizione 3.2.12. L'insieme di ramificazione Δ_E di una $\mathscr{M}(B)$-algebra étale coincide con l'intersezione degli insiemi $\Delta_{E,\zeta}$ al variare di ζ tra gli elementi primitivi di E come $\mathscr{M}(B)$-algebra.

3.3 Estensioni di $\mathbb{C}$ di grado di trascendenza 1

Nella sezione precedente abbiamo visto che c'è un'antiequivalenza tra le categorie $\mathfrak{V}_B$ e $\mathfrak{E}_B$ con B una superficie di Riemann compatta e connessa. In questa sezione vediamo che ogni superficie di Riemann compatta e connessa è un rivestimenti ramificato analitico finito della sfera di Riemann: da ciò segue che la categoria $\mathfrak{RS}$ delle superfici di Riemann compatte e connesse è equivalente alla categoria $\mathfrak{Tr}^1_{\mathbb{C}}$ delle estensioni di tipo finito di grado di trascendenza 1 di $\mathbb{C}$.

Indichiamo con $\mathbb{S}^2$ la sfera di Riemann, ossia la sfera munita di una struttura complessa in cui l'atlante analitico è dato dalle proiezioni stereografiche complesse rispetto ai due poli

$$\phi_0 : \mathbb{S}^2 \setminus \{\infty\} \to \mathbb{C} \quad , \quad \phi_1 : \mathbb{S}^2 \setminus \{0\} \to \mathbb{C}$$

con $\phi_0(z) = z$, $\phi_1(z) = \frac{1}{z}$ e $\phi_1(\infty) = 0$. Esiste un isomorfismo analitico tra la sfera di Riemann e la retta proiettiva complessa

$$\mathbb{S}^2 \cong \mathbb{P}^1(\mathbb{C})$$

Per comodità di notazione, scriveremo solo $\mathbb{P}^1$ in luogo di $\mathbb{P}^1(\mathbb{C})$.
Data una superficie di Riemann X, possiamo prolungare una funzione meromorfa $f : X \to \mathbb{C}$ ad una funzione $\tilde{f} : X \to \mathbb{P}^1$ mandando i poli di f nel valore ∞.

Proposizione 3.3.1. C'è una bigezione tra $\mathscr{M}(X)$ e l'insieme delle funzioni analitiche da X a $\mathbb{P}^1$ che non sono nè costanti nè uguali a ∞ su alcuna componente connessa di X, data da $f \mapsto \tilde{f}$.

Dimostrazione. Siano $f \in \mathscr{M}(X)$ e $x_0 \in X$. In un intorno di x_0, f è della forma $\frac{g}{h}$ con g, h olomorfe. Possiamo supporre che g e h non si annullano contemporaneamente in x_0. Se $h(x_0) \neq 0$ (risp. $g(x_0) \neq 0$), allora la funzione $\phi_0 \circ \tilde{f} = f$ (risp. $\phi_1 \circ \tilde{f} = \frac{h}{g}$) è olomorfa in un intorno di x_0. Segue che f è analitica.

Sia ora $h : X \to \mathbb{P}^1$ analitica. Poniamo $D = h^{-1}(\infty)$. Supponiamo che D non contenga alcuna componente connessa di X. Allora $f = \phi_0 \circ h : X \setminus D \to \mathbb{C}$ è meromorfa su X: infatti lo è su $X \setminus D$, e per ogni $x_0 \in D$ la funzione $g = \phi_1 \circ h$ è olomorfa e non identicamente nulla in un intorno di x_0 e si ha la funzione meromorfa $f = \frac{1}{g}$. □

Corollario 3.3.2. Sia X una superficie di Riemann compatta e connessa (non vuota). Allora X è un rivestimento ramificato analitico finito di $\mathbb{P}^1$.

Dimostrazione. Sia $f \in \mathscr{M}(X)$ non costante (esiste per il teorema di separazione 3.2.1). Prolunghiamo f alla funzione analitica $\tilde{f} : X \to \mathbb{P}^1$, che è un rivestimento ramificato analitico finito con ramificazione negli zeri e nei poli di f. □

Vogliamo ora caratterizzare le funzioni meromorfe su $\mathbb{P}^1$.
Un polinomio $P \in \mathbb{C}[Z]$ definisce una funzione $\mathbb{C} \to \mathbb{C}$ che è meromorfa su $\mathbb{P}^1$: infatti, è olomorfa su $\mathbb{C}$ e, in un intorno di ∞, la funzione $P \circ \phi_1 : z \mapsto P(\frac{1}{z})$ è una funzione razionale, dunque meromorfa. In generale, ogni funzione razionale definisce una funzione meromorfa su $\mathbb{P}^1$. Ma vale anche il viceversa, come afferma il risultato seguente (per una dimostrazione si rimanda a *Algebraic curves and Riemann surfaces* di R. Miranda [5, § 2.2.1]).

Teorema 3.3.3. Ogni funzione meromorfa su $\mathbb{P}^1$ è una funzione razionale, ossia

$$\mathscr{M}(\mathbb{P}^1) = \mathbb{C}(Z)$$

Una funzione razionale della forma $x \mapsto \dfrac{ax+b}{cx+d}$ con $ad-bc \neq 0$ definisce una funzione analitica $\mathbb{P}^1 \to \mathbb{P}^1$, detta *omografia*. Valgono i due seguenti fatti, che non dimostriamo:

1. $\mathrm{Aut}(\mathbb{P}^1) = \{f \in \mathbb{C}(Z) \ : \ f \text{ è omografia } \}$;
2. $\mathrm{Aut}(\mathbb{P}^1) = < x \mapsto x+b \ , \ x \mapsto ax \ , \ x \mapsto \frac{1}{x} >$.

Dai teoremi 3.3.3 e 3.2.9 abbiamo il seguente corollario.

Corollario 3.3.4. Sia $B = \mathbb{P}^1$. Esiste un'antiequivalenza di categorie tra i rivestimenti ramificati analitici finiti di $\mathbb{P}^1$ e le algebre étale su $\mathbb{C}(Z)$.

Il nostro intento è ora trovare una categoria equivalente alla categoria $\mathfrak{RS}$ delle superfici di Riemann compatte e connesse.
Per farlo, ricordiamo alcuni concetti della teoria dei campi.

Definizione. Sia F/K un'estensione di campi. Un elemento $x \in F$ è *trascendente* su K se non è algebrico. Una famiglia $(x_i)_I \subset F$ è detta *algebricamente libera* (e i suoi elementi *algebricamente indipendenti*) se l'omomorfismo $\varphi : K[(X_i)_I] \to F$ definito da $X_i \mapsto x_i$ è iniettivo. Una famiglia massimale di elementi di F algebricamente indipendenti su K è detta **base di trascendenza** di F su K. La cardinalità delle basi di trascendenza di F su K (si dimostra che queste hanno tutte la stessa cardinalità) è detta **grado di trascendenza** di F su K e la indichiamo con $\mathrm{trdeg}_K(F)$.

Ricordiamo inoltre che, se $(x_1, \dots, x_k)$ è una base di trascendenza di F su K, allora F è un'estensione algebrica di $K(x_1, \dots, x_k)$.

Il risultato che segue ci permetterà di ricorrere al teorema 3.2.9 per raggiungere i nostri scopi.

Proposizione 3.3.5. Sia X una superficie di Riemann compatta e connessa (non vuota). Allora $\mathscr{M}(X)$ è un'estensione di tipo finito di $\mathbb{C}$ di grado di trascendenza 1.

Dimostrazione. Sia $f \in \mathscr{M}(X)$ non costante (esiste per il teorema di separazione). Prolunghiamo f a $\tilde{f}$ e vediamo $(X, \tilde{f})$ come rivestimento ramificato analitico finito di $\mathbb{P}^1$. Allora, per il teorema 3.2.4, $\mathscr{M}(X)$ è un'estensione finita di $\mathscr{M}(\mathbb{P}^1) = \mathbb{C}(Z)$, e quindi $\mathrm{trdeg}_{\mathbb{C}}(\mathscr{M}(X)) = \mathrm{trdeg}_{\mathbb{C}}(\mathbb{C}(Z)) = 1$. $\square$

Indichiamo con $\mathfrak{Tr}^1_{\mathbb{C}}$ la categoria delle estensioni di tipo finito di $\mathbb{C}$ di grado di trascendenza 1.

Teorema 3.3.6. Il funtore $\mathscr{M} : \mathfrak{RS} \to \mathfrak{Tr}^1_{\mathbb{C}}$ è un'antiequivalenza di categorie.

Per la dimostrazione del teorema si rimanda a [9, § 6.3.5].

Corollario 3.3.7. La categoria delle superfici di Riemann compatte con morfismi le mappe analitiche non costanti su alcuna componente connessa è antiequivalente tramite il funtore $\mathscr{M}$ alla categoria delle $\mathbb{C}$-algebre che sono prodotto finito di estensioni di $\mathbb{C}$ di tipo finito di grado di trascendenza 1.

Dimostrazione. Basta ricordare che $\mathscr{M}(X \sqcup Y) = \mathscr{M}(X) \times \mathscr{M}(Y)$ e applicare il teorema precedente a ciascuna componente connessa. $\square$

Capitolo 4

Su due gruppi di Galois assoluti

4.1 Gruppo di Galois assoluto di $\mathbb{C}(Z)$

In questa sezione dimostriamo un risultato fondamentale che segue direttamente dall'antiequivalenza vista nel capitolo precedente tra le categorie $\mathfrak{Tr}^1_{\mathbb{C}}$ e $\mathfrak{RS}$: il gruppo di Galois assoluto di $\mathbb{C}(Z)$ è isomorfo al gruppo profinito libero $\hat{L}(\mathbb{C})$. Tale risultato risponde positivamente al problema inverso di Galois sul campo $\mathbb{C}(Z)$.

Diamo una semplice definizione preliminare.

Definizione. Siano K un campo e sia $\overline{K}$ una sua chiusura algebrica separabile. Il **gruppo di Galois assoluto** di K è il gruppo di Galois $\mathrm{Gal}(\overline{K}/K)$ della chiusura algebrica di K.

Vogliamo definire un omomorfismo che metta in relazione un gruppo fondamentale topologico con un gruppo di Galois algebrico.

Consideriamo una superficie di Riemann connessa e compatta B, un suo sottinsieme finito Δ e un elemento $b \in B \setminus \Delta$. Siano poi $E/\mathscr{M}(B)$ un'estensione di Galois finita tale che $\Delta_E \subset \Delta$ (per il luogo di ramificazione Δ_E cf. proposizione 3.2.12), e (X, π) un rivestimento ramificato analitico finito di B tale che l'isomorfismo

$$i : \mathscr{M}(X) \to E$$

identifichi queste due algebre. Siano $x \in \pi^{-1}(b) \subset X$ e $\Delta^{-1} = \pi^{-1}(\Delta)$.

Poichè $X \setminus \Delta^{-1}$ è un rivestimento di $B \setminus \Delta$, possiamo definire l'azione del gruppo fondamentale topologico $\pi_1(B \setminus \Delta, b)$ sulla fibra $\pi^{-1}(b)$. L'azione di monodromia di $\mathrm{Aut}_B(X)$ su $\pi^{-1}(b)$ è semplicemente transitiva, quindi per ogni $\gamma \in \pi_1(B \setminus \Delta, b)$ esiste (ed è unico) $g \in \mathrm{Aut}(X)$ tale che $g(x) = \gamma \cdot x$, dove con $\gamma \cdot x$ indichiamo il punto di arrivo $\gamma_x(1)$ del sollevamento γ_x del cammino γ.

Definiamo dunque l'omomorfismo

$$\begin{array}{rccc} \theta_x : & \pi_1(B \setminus \Delta, b) & \to & \mathrm{Gal}(E/\mathscr{M}(B)) \\ & \gamma & \mapsto & \theta_x(\gamma) = g^* \in \mathrm{Aut}(E) \end{array}$$

Vediamo che effettivamente è lineare. Se $\gamma, \gamma' \in \pi_1(B \setminus \Delta, b)$, denotiamo con g, g' i rispettivi automorfismi di X corrispondenti e con g'' l'automorfismo corrispondente a $\gamma \cdot \gamma'$: abbiamo $g''(x) = \gamma \cdot \gamma' \cdot x = \gamma \cdot g'(x) = g'(\gamma \cdot x) = \gamma'(g(x))$, da cui $g'' = g' \circ g$ e $\theta_x(\gamma \cdot \gamma') = g''^* = (g' \circ g)^* = g^* \circ g'^* = \theta_x(\gamma) \circ \theta_x(\gamma')$.

Notiamo che:

- θ_x è surgettivo e $\mathrm{Ker}\,\theta_x = \mathrm{Stab}_{\pi_1(B\setminus\Delta,b)}(x)$ è sottogruppo proprio di indice finito;
- θ_x dipende dalla scelta di x tra i punti della fibra $\pi^{-1}(b)$;
- dato $\gamma \in \pi_1(B \setminus \Delta, b)$, $\theta_x(\gamma)$ dipende unicamente dall'immagine di γ in $\pi_1(B \setminus \Delta_E, b)$ tramite il morfismo di gruppi fondamentali topologici indotto dall'inclusione $B \setminus \Delta \hookrightarrow B \setminus \Delta_E$.

Vediamo ora come si comporta l'omomorfismo θ_x rispetto ad un omomorfismo di algebre. Siano E, F due estensioni di Galois finite di $\mathscr{M}(B)$ con i rispettivi luoghi di ramificazione $\Delta_E, \Delta_F \subset \Delta$, e siano X, Y i corrispettivi rivestimenti ramificati analitici finiti di B, ossia tali che $\mathscr{M}(X) = E$ e $\mathscr{M}(Y) = F$. Sia $f : E \to F$ un omomorfismo di campi e sia $u : Y \to X$ l'unico B-morfismo tale che $u^* = f$. Siano $y \in \pi_Y^{-1}(b)$ e $x = u(y)$.

Proposizione 4.1.1. L'omomorfismo f è compatibile con le azioni definite da θ_x e θ_y, ossia per ogni $\gamma \in \pi_1(B \setminus \Delta, b)$ si ha il diagramma commutativo

$$\begin{tikzcd} F & F \arrow[l, "\theta_y(\gamma)"'] \\ E \arrow[u, "f"] & E \arrow[l, "\theta_x(\gamma)"] \arrow[u, "f"'] \end{tikzcd}$$

Dimostrazione. Poichè F è un'estensione di $\mathscr{M}(B)$, $Y \setminus \Delta^{-1}$ è rivestimento connesso di $B \setminus \Delta$. Consideriamo il diagramma

$$\begin{tikzcd} Y \arrow[r, "g_Y"] \arrow[d, "u"'] & Y \arrow[d, "u"] \\ X \arrow[r, "g_X"'] & X \end{tikzcd}$$

con $g_X \in \mathrm{Aut}_B(X)$ e $g_Y \in \mathrm{Aut}_B(Y)$ tali che $g_X(x) = \gamma \cdot x$ e $g_Y(y) = \gamma \cdot y$. Vediamo che il diagramma commuta su y, ossia $u(\gamma \cdot y) = \gamma \cdot u(y)$: posto $\tilde{\gamma}$ il sollevamento di γ in Y con origine y, si ha che $u \circ \tilde{\gamma}$ è il sollevamento del cammino γ in X con origine x e quindi

$$u(\gamma \cdot y) = u(\tilde{\gamma}(1)) = (u \circ \tilde{\gamma})(1) = \gamma \cdot u(y)$$

Dunque la tesi segue applicando il funtore $\mathscr{M}$ al diagramma sopra. □

Fissiamo B una superficie di Riemann compatta e connessa, Δ un suo sottinsieme finito e Ω una chiusura algebrica di $\mathscr{M}(B)$. Denotiamo con Ω_Δ l'unione di tutte le sottoestensioni di Galois finite $E \subset \Omega$ tali che $\Delta_E \subset \Delta$. Tale unione è filtrante, quindi Ω_Δ è una sottoestensione di Ω. Notiamo che:

- Ω_Δ è stabile per automorfismi di Ω (ossia è normale) poichè unione filtrante di estensioni normali con ramificazione nello stesso sottinsieme Δ;
- Ω_Δ è separabile poichè $char\mathscr{M}(B) = 0$.

Segue che $\Omega_\Delta/\mathscr{M}(B)$ è un'estensione di Galois. Inoltre, per ogni estensione di Galois finita $F/\mathscr{M}(B)$ contenuta in Ω_Δ si ha $\Delta_F \subset \Delta$.

Vogliamo determinare il gruppo di Galois di Ω_Δ.

Sia $(E_i)_i$ una famiglia filtrante di estensioni di Galois finite di $\mathscr{M}(B)$ tali che $\bigcup_i E_i = \Omega_\Delta$. Per ogni i identifichiamo E_i ad un'algebra della forma $\mathscr{M}(X_i)$ con X_i rivestimento ramificato analitico finito di B: $\forall i \leq j$ da $E_i \subset E_j$ si ha un B-morfismo $p_{i,j} : X_j \to X_i$ tale che $p_{i,j}^*$ è l'immersione canonica di E_i in E_j. Allora gli spazi X_i con i morfismi $p_{i,j}$ formano un sistema proiettivo di rivestimenti ramificati di B.
Dato $b \in B$, per ogni i indichiamo con $X_i(b)$ la fibra di b in X_i. Allora $\varprojlim X_i(b)$ è non vuoto, per il teorema di Tychonoff. Sia $x \in \varprojlim X_i(b)$: per ogni i denotiamo con $p_i(x)$ l'immagine di x in $X_i(b)$ e consideriamo l'omomorfismo $\theta_{p_i(x)}$. Passando al limite proiettivo otteniamo l'omomorfismo

$$\theta_x : \pi_1(B \setminus \Delta, b) \longrightarrow \mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B)) = \varprojlim \mathrm{Gal}(E_i/\mathscr{M}(B))$$

Poichè il gruppo $\mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$ è profinito, l'omomorfismo θ_x si estende (cf. Sez 1.2) in un omomorfismo continuo $\widehat{\theta}_x$ dal completamento profinito $\widehat{\pi}_1(B \setminus \Delta, b)$ di $\pi_1(B \setminus \Delta, b)$ in $\mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$.

Proposizione 4.1.2. L'omomorfismo $\widehat{\theta}_x : \widehat{\pi}_1(B \setminus \Delta, b) \to \mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$ è isomorfismo.

Dimostrazione. Sia $G = \pi_1(B \setminus \Delta, b)$. Supponiamo che la famiglia $(E_i)_i$ sia formata da tutte le sottoestensioni di Galois finite contenute in Ω_Δ. Per ogni i, sappiamo che il kernel dell'omomorfismo $\theta_{p_i(x)} : G \to \mathrm{Gal}(E_i/\mathscr{M}(B))$ è proprio lo stabilizzatore $N_i = \mathrm{Stab}_G(p_i(x))$: per il primo teorema di omomorfismo per gruppi, abbiamo quindi l'isomorfismo

$$h_i : G/N_i \to \mathrm{Gal}(E_i/\mathscr{M}(B))$$

Passando al limite proiettivo, otteniamo l'isomorfismo

$$h : \varprojlim G/N_i \to \mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$$

Sia $N < G$ un sottogruppo proprio di indice finito. Allora per la teoria dei rivestimenti sappiamo che esistono un rivestimento regolare finito (Y, π) di $B \setminus \Delta$ e un punto $y \in \pi^{-1}(b)$ tali che $\mathrm{Stab}_G(y) = N$. Completiamo quindi il rivestimento ad un rivestimento ramificato analitico $\widehat{Y}$ di B: allora $\mathscr{M}(\widehat{Y})$ è un'estensione di Galois di $\mathscr{M}(B)$ che possiamo considerare in Ω, dunque il Ω_Δ. Allora $\mathscr{M}(\widehat{Y})$ s'identifica ad un'estensione E_i e $N = N_i$.

Segue che $\varprojlim G/N_i$ è proprio il completamento profinito di G e che $h = \widehat{\theta_x}$, da cui $\widehat{\theta_x}$ è un isomorfismo. □

Vogliamo ora dare una descrizione del limite proiettivo

$$\mathrm{Gal}(\Omega/\mathscr{M}(B)) = \varprojlim \mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$$

al variare di Δ tra i sottinsiemi finiti di B. La difficoltà principale è data dalla scelta del punto base: infatti, fissato $b \in B$, non possiamo considerare i Δ contenenti b. Per bypassare questo problema una soluzione sta nel sostituire il punto base con un germe di cammini in B.

Sia $\beta : [0,1] \to B$ un cammino iniettivo. Per ogni $\Delta \subset B$ finito, consideriamo

$$c_\Delta = \sup\{c \in [0,1] \ : \ \beta(]0,c[) \subset B \setminus \Delta\}$$

e definiamo sull'insieme

$$\Lambda = \{(t,\gamma) \ : \ t \in]0, c_\Delta[\ , \ \gamma \in \pi_1(B \setminus \Delta, \beta(t))\}$$

la relazione d'equivalenza

$$(t_1,\gamma_1) \sim (t_2,\gamma_2) \iff \gamma_2 = (\beta|_{[t_1,t_2]})_\#(\gamma_1)$$

con $(\beta|_{[t_1,t_2]})_\#$ l'isomorfismo di gruppi

$$\begin{array}{rccc} (\beta|_{[t_1,t_2]})_\# : & \pi_1(B \setminus \Delta, \beta(t_1)) & \to & \pi_1(B \setminus \Delta, \beta(t_2)) \\ & [g] & \mapsto & [\beta|_{[t_1,t_2]} \circ g \circ \beta|_{[t_2,t_1]}] \end{array}$$

Definiamo allora il gruppo fondamentale relativo a un germe di cammini il gruppo

$$\pi_1(B \setminus \Delta, \beta) := \Lambda/\sim$$

e per ogni $t \in]0, c_\Delta[$ abbiamo l'isomorfismo canonico

$$\chi_t : \pi_1(B \setminus \Delta, \beta(t)) \longrightarrow \pi_1(B \setminus \Delta, \beta)$$

per cui possiamo dare una caratterizzazione del gruppo $\pi_1(B \setminus \Delta, \beta)$ come il limite induttivo $\varinjlim \pi_1(B \setminus \Delta, \beta(t))$ al variare di $t \in]0, c_\Delta[$: ciò segue dalla proposizione 1.2.4.

Siano dunque X un rivestimento ramificato analitico finito di B e $\Delta \subset B$ il suo insieme di ramificazione. Denotiamo con $\Gamma(\beta, X)$ l'insieme dei sollevamenti continui in X dei cammini $\beta|_{]0,c_\Delta[}$: se X è di grado d su B, l'insieme $\Gamma(\beta, X)$ ha d elementi. Supponiamo ora che X sia anche *regolare* come rivestimento di B. Sia $\zeta \in \Gamma(\beta, X)$.

Proposizione 4.1.3. Esiste uno ed unico omomorfismo

$$\theta_\zeta : \pi_1(B \setminus \Delta, \beta) \to \mathrm{Gal}(\mathscr{M}(X)/\mathscr{M}(B))$$

tale che per ogni $t \in]0, c_\Delta[$ si abbia $\theta_\zeta \circ \chi_t = \theta_{\zeta(t)}$.

Per la dimostrazione di tale risultato basta mostrare $\forall t < t' \in]0, c_\Delta[$ la commutatività del diagramma

$$\begin{tikzcd} \pi_1(B \setminus \Delta, \beta(t)) \arrow[d, "(\beta|_{[t,t']})_\#"'] \arrow[dr, "\theta_{\zeta(t)}"] & \\ & \mathrm{Gal}(\mathscr{M}(X)/\mathscr{M}(B)) \\ \pi_1(B \setminus \Delta, \beta(t')) \arrow[ur, "\theta_{\zeta(t')}"'] & \end{tikzcd}$$

Verifichiamo ora la funtorialità di θ_ζ.
Siano X, X' due rivestimenti ramificati analitici finiti regolari di B, Δ, Δ' i loro insiemi di ramificazione e $f : X' \to X$ un B-morfismo: abbiamo che f è surgettivo, $\Delta \subset \Delta'$ e $c_{\Delta'} \le c_\Delta$. Per ogni cammino risollevato $\zeta' \in \Gamma(\beta, X')$ esiste uno ed unico cammino risollevato $\zeta \in \Gamma(\beta, X)$ tale che $\zeta|_{]0,c_{\Delta'}[} = f \circ \zeta'$: indichiamo $\zeta = f_*(\zeta')$. Allora l'omomorfismo $f^* : \mathscr{M}(X) \to \mathscr{M}(X')$ è compatibile con le azioni di $\pi_1(B \setminus \Delta, \beta)$ definite da θ_ζ e $\theta_{\zeta'}$ (per la proposizione 4.1.1).

Abbiamo ora tutti gli strumenti per calcolare il gruppo di Galois assoluto del campo $\mathscr{M}(B)$ per qualche B superficie di Riemann compatta e connessa: fatto ciò saremo in grado di applicare il risultato a $B = \mathbb{P}^1$ e determinare il gruppo di Galois assoluto di $\mathbb{C}(Z)$.

Consideriamo Δ, Δ' due sottinsiemi finiti di B tali che $\Delta \subset \Delta'$. Allora per le proprietà dei rivestimenti esiste uno ed unico omomorfismo

$$r_{\Delta}^{\Delta'} : \pi_1(B \setminus \Delta', \beta) \to \pi_1(B \setminus \Delta, \beta)$$

che $\forall t \in]0, c_\Delta[$ rende commutativo il diagramma

$$\begin{tikzcd}
\pi_1(B \setminus \Delta', \beta(t)) \arrow[r, "i_*"] \arrow[d, "\chi_t"'] & \pi_1(B \setminus \Delta, \beta(t)) \arrow[d, "\chi_t"] \\
\pi_1(B \setminus \Delta', \beta) \arrow[r, "r_{\Delta}^{\Delta'}"'] & \pi_1(B \setminus \Delta, \beta)
\end{tikzcd}$$

Al variare di Δ nell'insieme filtrante dei sottinsiemi finiti di B, abbiamo il sistema proiettivo $(\pi_1(B \setminus \Delta, \beta), (r_{\Delta}^{\Delta'})_{\Delta \subset \Delta'})$ ed il rispettivo completamento profinito $(\widehat{\pi}_1(B \setminus \Delta, \beta), (\widehat{r}_{\Delta}^{\Delta'})_{\Delta \subset \Delta'})$.
Data Ω una chiusura algebrica di $\mathscr{M}(B)$ e $(E_i)_i$ una famiglia filtrante di tutte le sottoestensioni di Galois finite di Ω, poniamo $\Delta_i = \Delta_{E_i}$ l'insieme di ramificazione di ogni E_i. Identifichiamo quindi ciascun E_i con un'estensione del tipo $\mathscr{M}(X_i)$, con X_i rivestimento ramificato analitico finito di B. Per il teorema di Tychonoff, l'insieme $\Gamma = \varprojlim \Gamma(\beta, X_i)$ è non vuoto: sia dunque $\zeta = (\zeta_i) \in \Gamma$. Per ogni i l'omomorfismo

$$\theta_{\zeta_i} : \pi_1(B \setminus \Delta_i, \beta) \to \mathrm{Gal}(E_i/\mathscr{M}(B))$$

si estende per completamento profinito

$$\widehat{\theta}_{\zeta_i} : \widehat{\pi}_1(B \setminus \Delta_i, \beta) \to \mathrm{Gal}(E_i/\mathscr{M}(B))$$

Per la funtorialità di θ_ζ, per ogni $i \leq j$ si ha il diagramma commutativo

$$\begin{tikzcd}
\widehat{\pi}_1(B \setminus \Delta_j, \beta) \arrow[r, "\widehat{\theta}_{\zeta_j}"] \arrow[d, "\widehat{r}_{\Delta_i}^{\Delta_j}"'] & \mathrm{Gal}(E_j/\mathscr{M}(B)) \arrow[d, "\rho"] \\
\widehat{\pi}_1(B \setminus \Delta_i, \beta) \arrow[r, "\widehat{\theta}_{\zeta_i}"'] & \mathrm{Gal}(E_i/\mathscr{M}(B))
\end{tikzcd}$$

dove $\rho : \sigma \mapsto \sigma|_{E_i}$ è la restrizione (canonica). Passando al limite proiettivo, a partire dagli θ_{ζ_i} definiamo l'omomorfismo

$$\widehat{\theta}_\zeta : \varprojlim \widehat{\pi}_1(B \setminus \Delta, \beta) \to \mathrm{Gal}(\Omega/\mathscr{M}(B))$$

Possiamo ora determinare il gruppo di Galois assoluto di $\mathscr{M}(B)$.

Teorema 4.1.4. L'omomorfismo $\widehat{\theta}_\zeta : \varprojlim \widehat{\pi}_1(B \setminus \Delta, \beta) \to \mathrm{Gal}(\Omega/\mathscr{M}(B))$ è isomorfismo di gruppi profiniti.

Dimostrazione. Per ogni $\Delta \subset B$, denotiamo con ζ_Δ l'immagine di ζ nel limite proiettivo dei $\Gamma(\beta, X_i)$ per quegli i tali che $\Delta_i \subset \Delta$. Dall'identificazione $\pi_1(B \setminus \Delta, \beta) \cong \pi_1(B \setminus \Delta, \beta(t))$ e dalla proposizione 4.1.2, segue l'isomorfismo $\widehat{\theta}_{\zeta_\Delta} : \widehat{\pi}_1(B \setminus \Delta, \beta) \to \mathrm{Gal}(\Omega_\Delta/\mathscr{M}(B))$. Passando al limite proiettivo al variare di Δ, si ha la tesi. □

Siamo ora pronti per esplicitare il gruppo di Galois assoluto di $\mathbb{C}(Z)$. Fissiamo Ω una sua chiusura algebrica. Sia dunque $B = \mathbb{P}^1$ la sfera di Riemann.

Per ogni $\Delta \subset \mathbb{C}$ finito, poniamo $\overline{\Delta} = \Delta \cup \{\infty\} \subset \mathbb{P}^1$. Tali $\overline{\Delta}$ formano un insieme *cofinale* nell'insieme delle parti finite di $\mathbb{P}^1$, ossia per ogni Δ esiste un $\overline{\Delta'}$ tale che $\Delta \subset \overline{\Delta'}$. Da tale relazione segue che

$$\mathrm{Gal}(\Omega/\mathbb{C}(Z)) = \mathrm{Gal}(\Omega/\mathscr{M}(\mathbb{P}^1)) \cong \varprojlim \widehat{\pi}_1(\mathbb{P}^1 \setminus \overline{\Delta}, \beta) = \varprojlim \widehat{\pi}_1(\mathbb{C} \setminus \Delta, \beta)$$

dove β è un cammino iniettivo in $\mathbb{C}$.

Possiamo supporre che il cammino β intersechi ogni retta di $\mathbb{C}$ parallela all'asse reale solo un numero finito di volte, come ad esempio nel caso in cui β è un arco di circonferenza.

Resta dunque da determinare il gruppo profinito $\varprojlim \widehat{\pi}_1(\mathbb{C} \setminus \Delta, \beta)$. A tal scopo ricorriamo alla nozione di gruppo profinito libero costruito su un insieme (cf. Sez 1.2).

Proposizione 4.1.5. Sia $\widehat{L}(\mathbb{C})$ il gruppo profinito libero costruito su $\mathbb{C}$. Allora

$$\varprojlim \widehat{\pi}_1(\mathbb{C} \setminus \Delta, \beta) \cong \widehat{L}(\mathbb{C})$$

Dimostrazione. Dati $\Delta \in \mathbb{C}$ sottinsieme finito e $b \in \mathbb{C} \setminus \Delta$, il gruppo fondamentale topologico $\pi_1(\mathbb{C} \setminus \Delta, b)$ è isomorfo al gruppo libero $L(\Delta)$ costruito su Δ; allora anche $\pi_1(\mathbb{C} \setminus \Delta, \beta)$ è isomorfo a $L(\Delta)$.

Vogliamo determinare una base di $\pi_1(\mathbb{C} \setminus \Delta, \beta)$ per esplicitare tale isomorfismo. Consideriamo $a_1 \neq a_2 \in \Delta$ tali che b, a_1, a_2 non siano mai allineati e per ogni $a \in \Delta$ definiamo $\gamma_{b,a} \in \pi_1(\mathbb{C} \setminus \Delta, b)$ come la classe dei cammini che vanno in linea retta da b verso a, arrivati ad una certa distanza ϵ da a si fermano e descrivono un cerchio di

raggio ϵ intorno ad a e poi tornano in b in linea retta.
Poniamo inoltre $\epsilon \lneq |a' - a|$ per ogni $a' \in \Delta \setminus \{a\}$. Allora $(\gamma_{b,a})_{a\in\Delta}$ formano una base di $\pi_1(\mathbb{C} \setminus \Delta, b)$.

Definiamo quindi per ogni Δ una base $(\gamma_{\beta,a})_{a\in\Delta}$ di $\pi_1(\mathbb{C} \setminus \Delta, \beta)$. Ricordiamo che abbiamo supposto che β incontri ogni retta parallela all'asse reale in un numero finito di punti: in tal caso, esiste $c' \leq c_\Delta$ non nullo tale che $\beta(]0, c'[)$ non incontri alcuna retta congiungente due punti di Δ. Indichiamo con c'_Δ il più grande di tali c'. Poichè $t \in]0, c'_\Delta[$, la classe $\chi_t(\gamma_{\beta(t),a}) \in \pi_1(\mathbb{C} \setminus \Delta, \beta)$ è indipendente dalla scelta di t: la denotiamo quindi $\gamma_{\beta,a}$.

Per $\Delta \subset \Delta'$, l'omomorfismo $r_\Delta^{\Delta'} : \pi_1(\mathbb{C} \setminus \Delta', \beta) \to \pi_1(\mathbb{C} \setminus \Delta, \beta)$ è tale che

$$\gamma_{\beta,a} \mapsto \begin{cases} \gamma_{\beta,a} & \text{se } a \in \Delta \\ id & \text{se } a \notin \Delta \end{cases}$$

Si ha dunque il diagramma commutativo

$$\begin{tikzcd} L(\Delta') \arrow[r, "\alpha_{\Delta'}"] \arrow[d, "\rho_\Delta^{\Delta'}"'] & \pi_1(\mathbb{C} \setminus \Delta', \beta) \arrow[d, "r_\Delta^{\Delta'}"] \\ L(\Delta) \arrow[r, "\alpha_\Delta"'] & \pi_1(\mathbb{C} \setminus \Delta, \beta) \end{tikzcd}$$

dove l'omomorfismo $\rho_\Delta^{\Delta'}$ è quello definito nella Sez 1.2, mentre α_Δ è l'isomorfismo definito dalla base $(\gamma_{\beta,a})_{a\in\Delta}$.

Passando al completamento profinito e poi al limite induttivo al variare di Δ, si ottiene l'ismorfismo

$$\widehat{\alpha} : \widehat{L}(\mathbb{C}) \to \varprojlim \widehat{\pi}_1(\mathbb{C} \setminus \Delta, \beta)$$

□

A questo punto il teorema che segue è un semplice corollario dell'ultima proposizione.

Teorema 4.1.6. Il gruppo di Galois assoluto di $\mathbb{C}(Z)$ è isomorfo a $\widehat{L}(\mathbb{C})$.

Il risultato appena ottenuto è molto importante per rispondere (positivamente) al *problema inverso di Galois* su $\mathbb{C}(Z)$. Abbiamo infatti il corollario seguente.

Corollario 4.1.7. Ogni gruppo finito è isomorfo al gruppo di automorfismi di un'estensione finita di $\mathbb{C}(Z)$.

Dimostrazione. Sia G un gruppo finito di ordine n. Dividiamo la dimostrazione in due passaggi.

- Vediamo che G è quoziente di un gruppo libero.
  Sia $\{g_1, \dots, g_r\}$ un insieme di generatori per G. Consideriamo il gruppo libero $L(g_i)$ generato dall'insieme $\{g_1, \dots, g_r\}$: allora è ben definito l'omomorfismo surgettivo
  $$\begin{array}{rccc} \pi: & L(g_i) & \twoheadrightarrow & G \\ & g_i & \mapsto & g_i \end{array}$$
  Per il primo teorema di omomorfismo di gruppi, abbiamo che $G \cong L(g_i)/\operatorname{Ker}(\pi)$.

- Vediamo che per ogni insieme finito S esiste una surgezione dal gruppo libero $L(\mathbb{C})$ sul gruppo libero $L(S)$ generato da S.
  Vale il seguente fatto, per una cui dimostrazione si rimanda a [7, Sez I.12].

  Fatto. Per ogni funzione $f : \mathbb{C} \to S$, esiste un omomorfismo di gruppi $\tilde{f} : L(\mathbb{C}) \to L(S)$. Inoltre, se f è surgettiva, allora lo è anche $\tilde{f}$.

Per i due punti precedenti, abbiamo quindi un omomorfismo surgettivo di gruppi

$$\begin{tikzcd} L(\mathbb{C}) \arrow[r, two heads, "\tilde{f}"] \arrow[rr, bend right, two heads, "\psi"'] & L(g_i) \arrow[r, two heads, "\pi"] & G \end{tikzcd}$$

e, per il primo teorema di omomorfismo per gruppi, abbiamo $G \cong L(\mathbb{C})/\operatorname{Ker}(\psi)$. Inoltre, poichè G è finito, $\operatorname{Ker}(\psi)$ ha indice finito in $L(\mathbb{C})$. Dalla definizione del completamento profinito $\widehat{L}(\mathbb{C})$, segue che G è un sottogruppo di $\widehat{L}(\mathbb{C})$.
La tesi segue dalla corrispondenza di Galois nella teoria dei campi. □

4.2 *Dessins d'enfant*

Diamo ora una breve presentazione del teorema di Belyi, che ha importanti conseguenze nella teoria dei "dessins d'enfants" di Grothendieck, riducendo il problema della classificazione di particolari campi, detti "campi di numeri", a dei problemi di combinatoria. Questa sezione fornisce quindi un ponte con la teoria dei numeri: tuttavia non approfondiremo questo aspetto, ma mostreremo solo come quanto visto fin'ora trova applicazioni in questo ambito.

La teoria dei rivestimenti ramificati (unita ai risultati ottenuti in questa trattazione) trova applicazione anche nella teoria dei numeri. Un oggetto di particolare interesse in questo campo è il gruppo $\mathbb{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dove $\overline{\mathbb{Q}}$ denota la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Tale $\mathbb{G}$ è un gruppo profinito di cui non è stata ancora data una descrizione esplicita: infatti il *problema inverso di Galois* su $\mathbb{Q}$ è un problema ancora aperto.

L'obiettivo della teoria dei *dessins d'enfant* del matematico tedesco Alexander Grothendieck è di far agire $\mathbb{G}$ su degli insiemi finiti definiti combinatoriamente, per poter ottenere informazioni su $\mathbb{G}$ da questi ultimi.

Iniziamo a vedere qualche definizione.

Definizione. Un **campo di numeri** K è un'estensione finita di $\mathbb{Q}$.

Sia (S, π) un rivestimento ramificato analitico di $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{C})$ e sia $\mathscr{M}(S)$ la corrispondente algebra étale su $\mathbb{C}(Z)$. Se $\zeta \in \mathscr{M}(S)$ è un elemento primitivo dell'algebra con polinomio minimo $P(T) = T^d + a_{d-1}(Z)T^{d-1} + \cdots + a_0(Z) \in \mathbb{C}(Z)[T]$, allora l'algebra $\mathscr{M}(S)$ s'identifica all'algebra quoziente $\mathbb{C}(Z)[T]/(P)$. Inoltre, S è una compattificazione della superficie $S' = \{(x, y) \in \mathbb{C}^2 \ : \ x \in \mathbb{C} \setminus \Delta_{\mathscr{M}(S),\zeta} \ , \ P_x(y) = 0\}$ (cf. Sez 3.1).
Possiamo supporre che ogni a_i sia della forma $\frac{p_i}{q_i}$ con p_i, q_i coprimi in $\mathbb{C}[Z]$ e q_i monico: sia $b_d = \mathrm{lcm}(q_i)_i$. Poniamo $b_i = b_d a_i \in \mathbb{C}[Z]$ e $Q = b_d T^d + \cdots + b_0 \in \mathbb{C}[Z, T]$. Diciamo che Q è un **polinomio definente** per il rivestimento (S, π).

Definizione. Sia (S, π) un rivestimento ramificato analitico di $\mathbb{P}^1$ e sia K un sottocampo di $\mathbb{C}$. Il rivestimento è detto **definibile** su K se esiste un polinomio $Q \in K[Z, T]$ che sia definente per (S, π). Il rivestimento è detto **semi-definibile** su K se esistono un'estensione L/K finita in $\mathbb{C}$ ed un polinomio $Q \in L[Z, T]$ che sia definente per (S, π).

Definizione. Sia K un sottocampo di $\mathbb{C}$. Una superficie di Riemann compatta S è detta **definibile** (risp. **semi-definibile**) su K se esiste una funzione $f \in \mathscr{M}(S)$ non costante su alcuna componente connessa di S tale che il rivestimento ramificato analitico (S, f) sia definibile (risp. semi-definibile) su K.

Data S una superficie di Riemann compatta, indichiamo con $\mathscr{M}^*(S)$ l'insieme delle funzioni meromorfe su S non costanti su alcuna componente connessa di S. Data $f \in \mathscr{M}^*(S)$, denotiamo con $\Delta(f)$ l'insieme dei valori critici di f vista come funzione analitica $S \to \mathbb{P}^1$. Inoltre, consideriamo un polinomio $f \in \mathbb{C}[Z]$ come una funzione $\mathbb{P}^1 \to \mathbb{P}^1$.
Infine, per ogni K sottocampo di $\mathbb{C}$ indichiamo con $\overline{K}$ la sua chiusura algebrica in $\mathbb{C}$.

Definizione. Una superficie di Riemann compatta S è detta **aritmetica** se è semi-definibile su $\mathbb{Q}$, ossia se è definibile su un campo di numeri.

Negli anni '70, Grothendieck si chiese se fosse vero che ogni curva algebrica (i.e. ogni 1-varietà complessa compatta) fosse rappresentabile tramite polinomi a coefficienti in un campo di numeri. Una risposta giunse nel 1979 dal matematico ucraino G. V. Belyi, che enunciò (e dimostrò) il seguente teorema (per la cui dimostrazione si rimanda a [9, Sez 7.2]).

Teorema 4.2.1 (Teorema di Belyi)**.** Data S una superficie di Riemann compatta, sono equivalenti:

1. S è aritmetica;
2. $\exists f \in \mathscr{M}^*(S)$ tale che $\Delta(f) \subset \overline{\mathbb{Q}} \cup \{\infty\}$;
3. $\exists f \in \mathscr{M}^*(S)$ tale che $\Delta(f) \subset \{0, 1, \infty\}$.

Tale teorema afferma che ogni superficie di Riemann aritmetica può essere ottenuta come rivestimento ramificato della sfera di Riemann $\mathbb{P}^1$ con ramificazione *soltanto* in $0, 1$ e ∞ (quindi con ramificazione in esattamente tre punti).

Dal teorema 3.2.9 abbiamo un'antiequivalenza di categorie tra la categoria $\mathfrak{E}$ delle $\mathbb{C}(Z)$-algebre étale E tali che $\Delta_E \subset \{0, 1, \infty\}$, e la categoria $\mathfrak{V}$ dei rivestimenti ramificati analitici di $\mathbb{P}^1$ con ramificazione in $\{0, 1, \infty\}$, data dal funtore $\mathscr{M} : X \mapsto \mathscr{M}(X)$ che ad ogni rivestimento ramificato X associa la $\mathbb{C}(Z)$-algebra $\mathscr{M}(X)$.

Questo risultato ha importanti conseguenze in geometria aritmetica. Vediamo come il tutto termina in ambito combinatoriale. Un **dessin d'enfant** è un grafo bipartito, i cui vertici sono colorati alternativamente di bianco e di nero, immerso in una superficie di Riemann: grazie a Belyi, sappiamo che le superfici di Riemann in cui è possibile immergere tali grafi sono quelle aritmetiche, ossia quelle corrispondenti a curve algebriche definite su un campo di numeri. Il gruppo di Galois assoluto $\mathbb{G}$ di $\mathbb{Q}$ agisce su queste curve, quindi sui grafi. Dalle trasformazioni dei grafi è quindi possibile dedurre informazioni sul gruppo $\mathbb{G}$.

Bibliografia

[1] H. Cartan. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.* Hermann, 1961.

[2] S. Lubkin. Theory of covering spaces, *Transactions of the American Mathematical Society* **104**:205-238, 1962.

[3] A. Grothendieck. *Revêtements étales et groupe fondamental* (SGA 1) : Séminaire de géométrie algébrique du Bois-Marie 1960-61, Lecture Notes in Mathematics, 224, Springer-Verlag, 1971.

[4] R. Hartshorne. *Algebraic geometry.* Springer-Verlag New York, 1977.

[5] R. Miranda. *Algebraic curves and Riemann surfaces.* American Mathematical Society, 1995.

[6] F. Borceux, G. Janelidze. *Galois theories.* Cambridge University Press, 2001.

[7] S. Lang. *Algebra*, Springer-Verlag New York, 2002.

[8] S. Bosch. *Algebra.* Springer-Verlag Italia, 2003.

[9] R. Douady, A. Douady. *Algèbre et théorie galoisiennes.* Cassini, Paris, 2005.

[10] T. Szamuely. *Galois groups and fundamental groups*, Cambridge studies in advanced mathematics, Cambridge, 2009.

[11] D. Eriksson, U. Persson. Galois theory and coverings, *Normat* **59**(3):1–8, 2011.

[12] A. Fehm, D. Haran, E. Paran. The inverse Galois problem over $\mathbb{C}(Z)$. *Manuscript*, 2013.

[13] A. Khovanskii. *Topological Galois theory.* Springer-Verlag Berlin, 2014.