Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA
Corso di Laurea Triennale in Matematica

Relazione Prova Finale

Gruppi di Galois e Gruppi Fondamentali

Laureando:
Sebastiano Tronto
Matricola 166581

Supervisore:
Prof. E. Ballico

Anno Accademico 2015-2016

Indice

Introduzione

Nella sua formulazione classica, la Teoria di Galois fornisce un collegamento tra la teoria delle estensioni di campi e la teoria dei gruppi. Il Teorema Fondamentale (Teorema 2.1.6) ci dice che i campi intermedi ad un'estensione finita e di Galois sono in corrispondenza biunivoca con i sottogruppi del gruppo di automorfismi dell'estensione stessa. La corispondenza di Galois non si ferma qui: le inclusioni vengono rovesciate, i gradi delle estensioni intermedi coincidono con gli indici dei sottogruppi, i sottogruppi normali corrispondo ad estensioni di Galois, e molto altro ancora.

C'è una corrispondenza del tutto analoga tra i rivestimenti di uno spazio topologico connesso (che soddisfi opportune potesi di regolarità) e i sottogruppi del gruppo fondamentale di X. Non a caso il gruppo fondamentale è isomorfo al gruppo degli automorfismi del rivestimento universale di X (Proposizione 3.3.3). Formulando in maniera diversa la teoria di Galois dei campi, vedremo che quest'ultimo è l'analogo del gruppo di Galois della chiusura separabile di un campo.

Per Grothendieck, queste due teorie sono in realtà due aspetti di un'unica teoria più generale. In questa relazione, seguendo i primi tre capitoli del libro *Galois Groups and Fundamental Groups* di Tamás Szamuely, esploreremo alcuni aspetti di questa teoria. Dopo alcuni risultati e nozioni preliminari ricorderemo i risultati fondamentali della Teoria di Galois per estensioni finite, per poi concentrarci sul caso infinito. Quanto appena dimostrato verrà poi riformulato nel linguaggio di Grothendieck, tramite equivalenze di categorie.

Nella seconda parte verrà esposta la Teoria di Galois per rivestimenti di spazi topologici. Verranno date due riformulazioni tramite equivalenza di categorie: la prima, in analogia con il caso algebrico; la seconda, che utilizza i fasci localmente costanti, sarà utile in seguito. Infine, studiando il caso delle superfici di Riemann, si vedrà come le estensioni del campo delle funzioni meromorfe su una superficie corrispondano a rivestimenti ramificati della superficie stessa.

Gli argomenti trattati in questa relazione terminano qui, ma è possibile generalizzare questi risultati (si veda [9], Capitolo 5). La formulazione del Teorema Fondamentale nell'ambito della teoria degli schemi, dovuta a Grothendieck, permette di definire il gruppo fondamentale (algebrico) di uno schema. Inoltre, il caso algebrico delle estensioni di campi diventa un caso particolare di questa teoria, il caso $X = \operatorname{Spec} k$, per k un campo. C'è quindi una teoria più generale che unifica, in un unico linguaggio, il caso algebrico e quello geometrico.

1 Preliminari

1.1 Categorie

La Teoria delle Categorie è assiomatica. Diamo la seguente descrizione informale.

Definizione 1.1.1. Una *categoria* $\mathcal{C}$ è formata da una classe di oggetti, denotata con $\mathrm{Obj}(\mathcal{C})$ e, per ogni $A, B \in \mathrm{Obj}(\mathcal{C})$, un insieme $\mathrm{Hom}(A, B)$, detto insieme dei *morfismi* da A in B, tale che:

1. Per ogni $A \in \mathrm{Obj}(\mathcal{C})$, esiste un morfismo $\mathrm{id}_A \in \mathrm{Hom}(A, A)$, detto *identità* di A.

2. Per ogni $A, B, C \in \mathrm{Obj}(\mathcal{C})$ e $\varphi \in \mathrm{Hom}(A, B)$ e $\psi \in \mathrm{Hom}(B, C)$, esiste un morfismo $\psi \circ \varphi \in \mathrm{Hom}(A, C)$, detto *composizione* di φ e ψ.

3. Per ogni $A, B \in \mathrm{Obj}(\mathcal{C})$ e $\varphi \in \mathrm{Hom}(A, B)$ vale $\varphi \circ \mathrm{id}_A = \varphi = \mathrm{id}_B \circ \varphi$.

4. Per ogni $A, B, C, D \in \mathrm{Obj}(\mathcal{C})$ e $\varphi \in \mathrm{Hom}(A, B)$ e $\psi \in \mathrm{Hom}(B, C)$ e $\lambda \in \mathrm{Hom}(C, D)$ vale $\lambda \circ (\psi \circ \varphi) = (\lambda \circ \psi) \circ \varphi$.

Due oggetti A, B di una stessa categoria si dicono *isomorfi* se esistono morfismi $\varphi \in \mathrm{Hom}(A, B)$ e $\psi \in \mathrm{Hom}(B, A)$ tali che $\varphi \circ \psi = \mathrm{id}_B$ e $\psi \circ \varphi = \mathrm{id}_A$.

Una *sottocategoria* $\mathcal{D}$ di una categoria $\mathcal{C}$ è una categoria che ha come oggetti una sottocollezione di $\mathrm{Obj}(\mathcal{C})$ e come morfismi tra due oggetti A e B un sottoinsieme di $\mathrm{Hom}(A, B)$. Una sottocategoria $\mathcal{D}$ di $\mathcal{C}$ si dice *piena* se ogni morfismo in $\mathcal{C}$ tra oggetti di $\mathcal{D}$ è ance un morfismo in $\mathcal{D}$.

Data una categoria $\mathcal{C}$, la categoria opposta $\mathcal{C}^{op}$ consiste degli stessi oggetti ($\mathrm{Obj}(\mathcal{C}^{op}) = \mathrm{Obj}(\mathcal{C})$) e, per $A, B \in \mathrm{Obj}(\mathcal{C})$, l'insieme $\mathrm{Hom}(A, B)$ di $\mathcal{C}$ è in biiezione canonica con l'insieme $\mathrm{Hom}(B, A)$ di $\mathcal{C}^{op}$.

Si noti che, in particolare, non è richiesto che la collezione degli oggetti sia un insieme. Rimandiamo a [5], I.6 per una discussione sul rapporto con la teoria degli insiemi. Nel seguito spesso scriveremo $A \in \mathcal{C}$ al posto di $A \in \mathrm{Obj}(\mathcal{C})$.

Esempio 1.1.2.

1. Gli insiemi con le funzioni tra insiemi formano una categoria, che denotiamo con Set. Sono categorie anche spazi topologici con le mappe continue (Top) e i gruppi con i morfismi di gruppi (Grp).

2. I gruppi abeliani sono una sottocategoria piena di Grp. Gli anelli con unità, i cui morfismi preservano l'unità, formano una sottocategoria non piena della categoria degli anelli.

3. Sia $(A, \leq)$ un insieme parzialmente ordinato (con $\leq$ ordine "largo"). Una categoria $\mathcal{C}$ può essere ottenuta ponendo $\mathrm{Obj}(\mathcal{C}) = A$ e $\mathrm{Hom}(a, b) = \{(a, b)\}$ se $a \leq b$, $\mathrm{Hom}(a, b) = \emptyset$ altrimenti.

4. Sia (X, τ) uno spazio topologico. Allora τ è un insieme parzialmente ordinato dall'inclusione. Applicando l'esempio precedente a $(\tau, \subset)$ otteniamo una categoria, che denoteremo con X_{TOP}.

Definizione 1.1.3 (Funtore)**.** Siano $\mathcal{C}$ e $\mathcal{D}$ due categorie. Un *funtore covariante* F tra $\mathcal{C}$ e $\mathcal{D}$, denotato con $F : \mathcal{C} \to \mathcal{D}$, è dato da una regola che associa ad ogni oggetto $A \in \mathcal{C}$ un oggetto $F(A) \in \mathcal{D}$ e ad ogni morfismo $\varphi \in \mathrm{Hom}(A, B)$ un morfismo $F(\varphi) \in \mathrm{Hom}(F(A), F(B))$, per ogni $A, B \in \mathcal{C}$, tale che $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ e $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$. Un *funtore controvariante* tra $\mathcal{C}$ e $\mathcal{D}$ è un funtore covariante tra $\mathcal{C}$ e $\mathcal{D}^{op}$.

Un funtore, covariante o controvariante, è detto *fedele* (rispettivamente *pieno*, *pienamente fedele*) se ogni mappa tra i morfismi $\varphi \mapsto F(\varphi)$ è iniettiva (rispettivamente suriettiva, biiettiva). Un funtore $F : \mathcal{C} \to \mathcal{D}$ è detto *essenzialmente suriettivo* se ogni $B \in \mathcal{D}$ è isomorfo a $F(A)$ per qualche $A \in \mathcal{C}$.

Un funtore covariante (rispettivamente controvariante) pienamente fedele ed essenzialmente suriettivo è detto *equivalenza* (rispettivamente *anti-equivalenza*) di categorie.

Definizione 1.1.4. Siano $\mathcal{C}$ e $\mathcal{D}$ due categorie e F e G due funtori tra $\mathcal{C}$ e $\mathcal{D}$. Un *morfismo* Φ tra F e G è dato da morfismi $\Phi_A : F(A) \to G(A)$ di $\mathcal{D}$, per ogni $A \in \mathcal{C}$, tali che per ogni morfismo $\varphi \in \mathrm{Hom}(A, B)$ in $\mathcal{C}$ commuti il seguente diagramma:

$$\begin{tikzcd} F(A) \arrow[r, "\Phi_A"] \arrow[d, "F(\varphi)"'] & G(A) \arrow[d, "G(\varphi)"] \\ F(B) \arrow[r, "\Phi_B"] & G(B) \end{tikzcd} \tag{1}$$

Osservazione 1.1.5. Fissate due categorie $\mathcal{C}$ e $\mathcal{D}$, i funtori tra di esse formano una categoria. Notiamo inoltre che un morfismo $\Phi : F \to G$ come nella definizione precedente è un isomorfismo (cioè: esiste $\Psi : G \to F$ tale che $\Phi \circ \Psi = \mathrm{id}_G$ e $\Psi \circ \Phi = \mathrm{id}_F$) se e solo se ognuno dei Φ_A è un isomorfismo.

Il seguente Lemma si generalizza immediatamente ai funtori cotrovarianti e alle anti-equivalenze.

Lemma 1.1.6. *Siano $\mathcal{C}$ e $\mathcal{D}$ due categorie e $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{C}$ funtori covarianti. Se esistono isomorfismi (nelle categorie dei funtori da $\mathcal{C}$ a $\mathcal{C}$ e da $\mathcal{D}$ a $\mathcal{D}$) $\Phi : G \circ F \to \mathrm{id}_{\mathcal{C}}$ e $\Psi : F \circ G \to \mathrm{id}_{\mathcal{D}}$ allora $\mathcal{C}$ e $\mathcal{D}$ sono categorie equivalenti.*

Dimostrazione. Il funtore F è essenzialmente suriettivo, perché qualunque $D \in \mathcal{D}$ è isomorfo a $F(G(D))$ tramite Ψ_D. Dati $A, B \in \mathcal{C}$, se consideriamo le mappe sui morfismi

$$\mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(F(A), F(B)) \longrightarrow \mathrm{Hom}(G(F(A)), G(F(B))) \longrightarrow \mathrm{Hom}(A, B)$$

indotte da F, G e Φ rispettivamente, abbiamo che la loro composizione è l'identità, quindi in particolare la mappa indotta da F è iniettiva e abbiamo che F è fedele. Similmente si verifica che G è fedele. Per $g \in \mathrm{Hom}(F(A), F(B))$, posto $f := \Phi_B \circ G(g) \circ \Phi_A^{-1}$ da $f = \Phi_B \circ G(F(f)) \circ \Phi_A^{-1}$ si ha $G(g) = G(F(f))$ quindi, poiché G è fedele, vale $g = F(f)$ e F è anche pieno. □

In realtà la condizione sufficiente del Lemma è anche necessaria e viene in alcuni casi data come definizione di equivalenza di categorie (si veda [9], sezione 1.5 e [5], IV.4, Theorem 1).

1.2 Limiti

Definizione 1.2.1. Un insieme parzialmente ordinato $(\Lambda, \leq)$ è detto *filtrato* se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Esempio 1.2.2. Sia $\mathcal{N}$ un sistema fondamentale di intorni di uno spazio topologico. Definiamo una relazione $\leq$ su $\mathcal{N}$ ponendo $N \leq M \iff N \supset M$ per ogni $N, M \in \mathcal{N}$. Allora $(\mathcal{N}, \leq)$ è un insieme parzialmente ordinato filtrato.

Definizione 1.2.3. Sia $\mathcal{I}$ la categoria determinata da un ordine parziale filtrato $(I, \leq)$ (terzo esempio di 1.1.2) e sia $\mathcal{C}$ una categoria. Un funtore covariante (rispettivamente controvariante) $F : \mathcal{I} \to \mathcal{C}$ è detto *sistema diretto* (rispettivamente *sistema inverso*) di oggetti di $\mathcal{C}$. Per $i, j \in I$, indicheremo con A_i l'oggetto $F(i)$ di $\mathcal{C}$ e con φ_{ij} il morfismo $F((i, j))$ da A_i ad A_j (rispettivamente da A_j ad A_i). Il sistema diretto (o inverso) verrà denotato da $(A_i, \varphi_{ij})_{i \in I}$, a volte omettendo l'indice.

Definizione 1.2.4 (Limiti diretti e inversi)**.** Sia $(A_i, \varphi_{ij})_{i \in I}$ un sistema diretto in una categoria $\mathcal{C}$. Un elemento $G \in \mathcal{C}$ con morfismi $f_i : A_i \to G$ per ogni $i \in I$ che facciano commutare i diagrammi

$$\begin{tikzcd} A_i \arrow[r, "\varphi_{ij}"] \arrow[dr, "f_i"'] & A_j \arrow[d, "f_j"] \\ & G \end{tikzcd} \tag{2}$$

per ogni $i \leq j$, tale che, per ogni $D \in \mathcal{C}$ con morfismi $g_i : A_i \to D$ che facciano commutare il diagramma, esista un unico morfismo $\psi : G \to D$ tale che $g_i = \psi \circ f_i$ per ogni $i \in I$, è detto *limite diretto* del sistema (A_i, φ_{ij}) ed è denotato da $\varinjlim_{i \in I} A_i$.

Sia $(A_i, \varphi_{ij})_{i \in I}$ un sistema inverso in una categoria $\mathcal{C}$. Un elemento $G \in \mathcal{C}$ con morfismi $f_i : G \to A_i$ per ogni $i \in I$ che facciano commutare i diagrammi

$$\begin{tikzcd} G \arrow[d, "f_i"'] \arrow[dr, "f_j"] & \\ A_i \arrow[r, "\varphi_{ji}"'] & A_j \end{tikzcd} \tag{3}$$

per ogni $j \leq i$, tale che, per ogni $D \in \mathcal{C}$ con morfismi $g_i : D \to A_i$ che facciano commutare il diagramma, esista un unico morfismo $\psi : D \to G$ tale che $g_i = f_i \circ \psi$ per ogni $i \in I$, è detto *limite inverso* del sistema (A_i, φ_{ij}) ed è denotato da $\varprojlim_{i \in I} A_i$.

Spesso ometteremo i pedici e indicheremo i limiti diretti e inversi con $\varinjlim A_i$ e $\varprojlim A_i$ rispettivamente. Avendo dato la definizione tramite proprietà universale, si ha immediatamente che un limite (diretto o inverso), se esiste, è unico a meno di un unico isomorfismo. Diamo ora due costruzioni dirette dei limiti in due casi concreti. Per dimostrare che questi oggetti sono effettivamente i limiti dichiarati, basta verificare che essi soddisfano le proprietà universali, si veda [3], Chapter 6, Proposition 2.4 per il caso dei gruppi.

Esempio 1.2.5. Se (A_i, φ_{ij}) è un sistema diretto di insiemi, $\varinjlim A_i$ può essere interpretato come l'unione disgiunta degli A_i modulo la relazione d'equivalenza così definita: $a_i \in A_i$ e $a_j \in A_j$ sono equivalenti se e solo se $\varphi_{ik}(a_i) = \varphi_{jk}(a_j)$ per qualche $k \geq i, j$. Le mappe $A_j \to \varinjlim A_i$ sono date dalla composizione di inclusioni canoniche e passaggio al quoziente.

Esempio 1.2.6. Se $(G_i, \varphi_{ij})_{i \in I}$ è un sistema inverso di gruppi (o di gruppi topologici, si veda la sezione 1.3), $\varprojlim G_i$ è isomorfo al sottogruppo del prodotto diretto $\prod_{i \in I} G_i$ dato da $\{(g_i)_{i \in I} \mid \varphi_{ij}(g_j) = g_i \ \forall i \leq j\}$. Le mappe $\varprojlim G_i \to G_j$ sono le proiezioni canoniche.

1.3 Gruppi Topologici e Gruppi Profiniti

Definizione 1.3.1. Un *gruppo topologico* è un gruppo G dotato di una topologia tale che le mappe

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\mapsto ab \end{aligned} \qquad\qquad \begin{aligned} \cdot^{-1} : G &\to G \\ a &\mapsto a^{-1} \end{aligned}$$

siano continue (dove $G \times G$ ha la topologia prodotto). Un morfismo di gruppi topologici è un morfismo (rispetto alla struttura di gruppo) continuo (rispetto alla topologia).

Notiamo che le mappe di moltiplicazione e di inversione sono sempre anche aperte. Inoltre, ogni sottogruppo (rispettivamente quoziente) di un gruppo topologico è ancora un gruppo topologico, se dotato della topologia indotta (rispettivamente quoziente). È possibile dare ad un qualunque gruppo una struttura di gruppo topologico dotandolo della topologia discreta.

Definizione 1.3.2. Un *gruppo profinito* è un gruppo topologico G per cui esiste un sistema inverso di gruppi topologici finiti e discreti (G_i, φ_{ij}) tale che $G = \varprojlim G_i$.

Un gruppo profinito può essere caratterizzato dalla stessa costruzione dell'Esempio 1.2.6. La topologia di un gruppo profinito è quindi quella indotta dal prodotto dei gruppi finiti di cui è limite.

Lemma 1.3.3. *Sia (G_i, φ_{ij}) un sistema inverso di gruppi topologici, con i G_i finiti e discreti. Allora $G = \varprojlim G_i$ è chiuso in $P = \prod G_i$.*

Dimostrazione. Sia $g = (g_i) \in P \setminus G$ e siano quindi i e j tali che $\varphi_{ij}(g_j) \neq g_i$. Poniamo $U := \{(h_i) \in P \,|\, h_i = g_i \text{ e } h_j = g_j\}$. Chiaramente $g \in U$ e $U \cap G = \emptyset$. Resta da verificare che U è aperto. Dette $p_k : P \to G_k$ le proiezioni canoniche, si ha che $U = p_i^{-1}(\{g_i\}) \cap p_j^{-1}(\{g_j\})$ ed è quindi aperto perché le proiezioni sono continue e i G_i discreti. □

Proposizione 1.3.4. *Un gruppo profinito G è compatto. I sottogruppi aperti di G sono tutti e soli i suoi sottogruppi chiusi di indice finito. I sottogruppi chiusi di G sono intersezione di sottogruppi aperti. I sottogruppi chiusi e normali di G sono intersezione di sottogruppi aperti normali.*

Dimostrazione. Dato che gli spazi finiti sono compatti, per il teorema di Tychonoff lo è anche il loro prodotto. Allora G è, per il Lemma precedente, un sottoinsieme chiuso di uno spazio compatto, quindi è a sua volta compatto.

Un sottogruppo aperto U di G è chiuso, perché il suo complementare è unione delle sue classi laterali gU, che sono aperte perché la moltiplicazione per elementi di G è un omeomorfismo. Queste devono essere in numero finito per compattezza di G. Viceversa, se U è un sottogruppo chiuso di indice finito è il complementare dell'unione finita delle sue classi laterali, che sono chiuse, quindi è aperto.

Sia H un sottogruppo chiuso di G. Siano $\{G_i\}_{i \in I}$ tali che $G = \varprojlim_{i \in I} G_i$, $\pi_i : G \to G_i$ le proiezioni naturali e $\{U_j\}_{j \in J}$ la famiglia di tutti i sottogruppi aperti normali di G. Allora $\{\ker \pi_i\}_{i \in I} \subset \{U_j\}_{j \in J}$ e dalla costruzione di G si vede che $\bigcap_{j \in J} U_j \subset \bigcap_{i \in I} \ker \pi_i = \{1\}$, quindi $\bigcap_{j \in J} U_j = \{1\}$. Inoltre $HU_j = \{hu \,|\, h \in H,\, u \in U_j\}$ è un sottogruppo aperto di G per ogni $j \in J$, normale se H lo è. Vale $H = \bigcap_{j \in J} HU_j$: certamente $H = H \bigcap_{j \in J} U_j \subset \bigcap_{j \in J} HU_j$. Per l'altra inclusione, sia $g \in \bigcap_{j \in I} HU_j$. Se per assurdo fosse $g \notin H$ allora $1 \notin Hg \implies Hg \cap \bigcap_{j \in J} U_j = \emptyset \implies (Hg)^c \cup \bigcup_{j \in J} U_j^c = G$. Per compattezza di G esiste $J_0 \subset J$ finito tale che $(Hg)^c \cup \bigcup_{j \in J_0} U_j^c = G \implies Hg \cap \bigcap_{j \in J_0} U_j = \emptyset$. Ma $N := \bigcap_{j \in J_0} U_j$ è ancora un sottogruppo aperto e normale di G, quindi per ipotesi $g \in HN$. Esistono quindi $h \in H$ e $n \in N$ tali che $g = hn$. Ma allora $Hg \ni h^{-1}g = n \in N$, quindi $H \cap N \neq \emptyset$, assurdo. □

Lemma 1.3.5. *Sia $G = \varprojlim_{i \in I} G_i$ un gruppo profinito e siano $\pi_i : G \to G_i$ le suriezioni naturali. Allora $\{\ker \pi_i\}_{i \in I}$ è un sistema fondamentale di intorni di $1 \in G$.*

Dimostrazione. Indichiamo con $p_i : \prod G_i \to G_i$ le proiezioni canoniche. Per la definizione di topologia prodotto e discretezza dei G_i abbiamo che gli insiemi della forma $\bigcap_{i \in I_0} \ker p_i$ per qualche sottoinsieme finito I_0 di I formano un sistema fondamentale di intorni di 1 in $\prod G_i$. Quindi un sistema fondamentale di intorni di 1 in G è dato dagli insiemi della forma $G \cap \bigcap_{i \in I_0} \ker p_i = \bigcap_{i \in I_0} G \cap \ker p_i = \bigcap_{i \in I_0} \ker \pi_i$. Fissato uno di questi insiemi, dato che I è filtrato I_0 è finito, esiste $j \in I$ tale che $j \geq i$ per ogni $i \in I_0$. Si ha quindi che $\ker \pi_j \subset \ker \pi_i$ per ogni $i \in I_0$, da cui $\ker \pi_j \subset \bigcap_{i \in I_0} \ker \pi_i$. Concludiamo che anche $\{\ker \pi_j\}_{j \in I}$ è un sistema fondamentale di intorni di 1 in G. □

Definizione 1.3.6. Sia G un gruppo e sia Λ l'insieme dei suoi sottogruppi normali di indice finito. Per $N, M \in \Lambda$ con $N \subset M$ sia $\pi_{MN} : G/N \to G/M$ la mappa naturale di passaggio al quoziente. Allora $(G/N, \pi_{MN})_{N \in \Lambda}$ è un sistema inverso. Il limite $\hat{G} := \varprojlim_{\Lambda} G/N$, dove i quozienti finiti G/N si intendono dotati della topologia discreta, è detto *completamento profinito* di G.

1.4 Azioni di Gruppi e G-spazi

Definizione 1.4.1. Siano G un gruppo e $X \neq \emptyset$ un insieme. Un'*azione sinistra* di G su X è una mappa

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

tale che $1x = x$ per ogni $x \in X$ e $g(hx) = (gh)x$ per ogni $g, h \in G, x \in X$. Lo *stabilizzatore* di $x \in X$ è il sottogruppo $G_x := \{g \in G \,|\, gx = x\}$ di G, mentre la sua *orbita* è il sottoinsieme $Gx := \{gx \,|\, g \in G\}$ di X. L'azione è detta *transitiva* se esiste un'unica orbita.

Un insieme equipaggiato con un'azione di un gruppo G è detto *G-insieme sinistro*. Un *morfismo* tra due G-insiemi sinistri X ed Y è una mappa $f : X \to Y$ tale che $f(gx) = gf(x)$ per ogni $x \in X$ e $g \in G$. I G-insiemi sinistri con i rispettivi morfismi formano una categoria.

In maniera del tutto analoga si definiscono le azioni destre e i G-insiemi destri.

Proposizione 1.4.2. *Sia X un G-insieme sinistro con azione di G transitiva e sia $x \in X$. Allora X è isomorfo (come G-insieme sinistro) all'insieme della classi laterali di G_x in G con l'azione di G per moltiplicazione sinistra $(g, hG_x) \mapsto ghG_x$.*

Dimostrazione. Si veda [6], Theorem 4.20. □

Definizione 1.4.3. Siano G un gruppo topologico e X un insieme. Diciamo che un'azione di G su X è *continua* se, dotando X della topologia discreta, lo è la corrispondente mappa $G \times X \to X$.

Lemma 1.4.4. *Siano G un gruppo topologico e X un G-insieme. Allora l'azione di G su X è continua se e solo se ogni stabilizzatore è aperto in G.*

Dimostrazione. Sia $f : G \times X$ la mappa $(g, x) \mapsto gx$. Supponiamo che gli stabilizzatori siano aperti e dimostriamo che $f^{-1}(x)$ è aperto per ogni $x \in X$. Si ha $f^{-1}(x) = \{(g, y) \in G \times X \,|\, gy = x\} = \bigcup_{y \in X} \mathcal{G}_y$, dove $\mathcal{G}_y = \{(g, y) \in G \times \{y\} \,|\, gy = x\}$. Ognuno dei $\mathcal{G}_y$ è omeomorfo allo stabilizzatore G_x di x: fissato $h \in G$ tale che $hy = x$ si ha che la mappa $g \mapsto (gh, y)$ è un omeomorfismo da G_x in $\mathcal{G}_y$. Quindi $f^{-1}(x) = \bigcup_{y \in X} \mathcal{G}_y$ è aperto. Viceversa, se f è continua allora per $x \in X$ lo stabilizzatore G_x è aperto, perché controimmagine della mappa continua $f \circ i_x$, dove $i_x : G \to G \times X$ è definita ponendo $i_x(g) := (g, x)$. □

Definizione 1.4.5. Siano G un gruppo e X uno spazio topologico. Diciamo che X è un *G-spazio* se è un G-insieme sinistro tale che le mappe $x \mapsto gx$ siano continue per ogni $g \in G$. Se X è un G-spazio, l'azione di G è detta *propriamente discontinua* se ogni punto di X ha un intorno aperto U tale che $gU \cap U = \emptyset$ per ogni $1 \neq g \in G$.

Se X è un G-spazio le mappe $x \mapsto gx$ sono omeomorfismi di X in se stesso, con inversa $x \mapsto g^{-1}x$.

Definizione 1.4.6. Sia X un G-spazio. Denotiamo con X/G l'insieme delle orbite di X rispetto all'azione di G e con $p : X \to X/G$ la mappa di passaggio al quoziente. L'insieme X/G dotato della topologia quoziente rispetto a p è detto *spazio quoziente di X rispetto a G*. Si può verificare che la mappa di passaggio al quoziente $p : X \to X/G$ è sempre aperta (si vedano ad esempio le Proposizioni 3.1.4 e 3.2.2).

1.5 Fasci

Definizione 1.5.1. Sia (X, τ) uno spazio topologico. Un *prefascio* su X è un funtore controvariante $\mathcal{F} : X_{\text{TOP}} \to \text{SET}$. Per $U \subset V$ aperti di X, gli elementi di $\mathcal{F}(U)$ sono detti *sezioni* su U e le mappe tra insiemi $\mathcal{F}((U, V)) : \mathcal{F}(V) \to \mathcal{F}(U)$ sono dette *restrizioni* e sono indicate con res_{VU}. Se $s \in \mathcal{F}(V)$, indicheremo con $s_{|V}$ l'elemento $\text{res}_{VU}(s)$ di $\mathcal{F}(U)$.

Un *fascio* $\mathcal{F}$ su X è un prefascio che, per ogni aperto non vuoto U e ogni famiglia $\mathcal{U}$ di aperti non vuoti tale che $\bigcup \mathcal{U} = U$, soddisfi i seguenti due assiomi:

1. Se due sezioni $s, t \in \mathcal{F}(U)$ sono tali che $s_{|V} = t_{|V}$ per ogni $V \in \mathcal{U}$, allora $s = t$.

2. Data una famiglia di sezioni $\{s_V \in \mathcal{F}(V) \,|\, V \in \mathcal{U}\}$ tali che per ogni $V, W \in \mathcal{U}$ con $V \cap W \neq \emptyset$ si abbia $s_{V|V \cap W} = s_{W|V \cap W}$, esiste un $s \in \mathcal{F}(U)$ tale che $s_{|V} = s_V$ per ogni $V \in \mathcal{U}$.

Gli oggetti appena definiti vengono solitamente detti (pre)fasci *di insiemi*. Similmente si possono definire fasci di anelli, o di gruppi abeliani, o altro.

Osservazione 1.5.2. I prefasci su uno spazio topologico X formano una categoria i cui morfismi sono i morfismi di funtori. I fasci su X ne sono una sottocategoria piena.

Definizione 1.5.3. Siano X uno spazio topologico localmente connesso e $\mathcal{F}$ un prefascio su X. Allora fissato $x \in X$ e detto $(\Lambda, \leq)$ l'insieme parzialmente ordinato di tutti gli intorni aperti di x, dove $V \leq U \iff V \supset U$, si ha che $(\mathcal{F}(U), \mathrm{res}_{VU})_{U \in \Lambda}$ è un sistema diretto di insiemi. Il limite $\mathcal{F}_x := \varinjlim_{\Lambda} \mathcal{F}(U)$ è detto *spiga* di $\mathcal{F}$ in x.

La spiga è caratterizzata dalla costruzione data nell'Esempio 1.2.5. Utilizzando questa costruzione esplicita, dato un morfismo $f : \mathcal{F} \to \mathcal{G}$ di prefasci su X possiamo definire una mappa $f_x : \mathcal{F}_x \to \mathcal{G}_x$ ponendo $f_x([s]) := [f_U(s)]$, dove U è un intorno aperto di x, $s \in \mathcal{F}(U)$ e $f_U : \mathcal{F}(U) \to \mathcal{G}(U)$ è come nella Definizione 1.1.4. Questa mappa è ben definita proprio per la definizione di morfismo di funtori. Abbiamo quindi che $\mathcal{F} \mapsto \mathcal{F}_x$ è un funtore dalla categoria dei prefasci su X a Set.

Definizione 1.5.4. Siano X uno spazio topologico e S uno spazio discreto. Il *fascio costante* $\mathcal{F}_S$ è definito ponendo, per $U \subset X$ aperto, $\mathcal{F}_S(U) := \{f : U \to S \mid f \text{ continua}\}$. Un fascio $\mathcal{F}$ su X è detto *localmente costante* se ogni punto di X ha un intorno aperto U tale che la restrizione di $\mathcal{F}$ ad U sia isomorfa, nella categoria dei fasci su U, ad un fascio costante.

2 Teoria di Galois

Nella prima parte del capitolo verranno ricordati alcuni risultati fondamentali della teoria di Galois, in particolare nel caso delle estensioni finite. Nella seconda parte il Teorema Fondamentale verrà esteso al caso infinito, mentre nell'ultima verrà riformulato come anti-equivalenza di categorie.

2.1 Definizioni e Risultati Fondamentali

Definizione 2.1.1. Un'estensione di campi $L|k$ è detta *algebrica* se ogni $\alpha \in L$ è algebrico su k, cioè se esiste $p \in k[x]$ tale che $p(\alpha) = 0$. È detta *separabile* se il polinomio minimo su k di ogni elemento di L ha radici distinte in una chiusura algebrica di k. È detta *normale* se il polinomio minimo su k di ogni elemento di L ha tutte le sue radici in L.

Definizione 2.1.2. Sia $L|k$ un'estensione di campi. Denotiamo con $\mathrm{Aut}(L|k)$ il gruppo di automorfismi di L come k-algebra, cioè gli isomorfismi $f : L \to L$ tali che $f_{|k} = \mathrm{id}_k$. L'estensione $L|k$ è detta *di Galois* se ogni $\alpha \in L$ tale che $f(\alpha) = \alpha$ per ogni $f \in \mathrm{Aut}(L|k)$ è tale che $\alpha \in k$. In tal caso, poniamo $\mathrm{Gal}(L|k) := \mathrm{Aut}(L|k)$.

Teorema 2.1.3 (Elemento primitivo)**.** *Sia $L|k$ un'estensione separabile finita. Allora esiste un elemento $\alpha \in L$* primitivo*, cioè tale che $L = k(\alpha)$.*

Dimostrazione. Si veda [3], Chapter 2, Corollary 2.21. □

Proposizione 2.1.4. *Un'estensione algebrica è di Galois se e solo se è normale e separabile. Un'estensione $L|k$ è finita e di Galois se e solo se $|\mathrm{Aut}(L|k)| = [L : k]$ e se e solo se L è il campo di spezzamento di un polinomio separabile a coefficienti in k.*

Sia inoltre $K|k$ un estensione di Galois con $K \supset L$. Allora $L|k$ è di Galois se e solo se $\sigma(L) \subset L$ per ogni $\sigma \in \mathrm{Gal}(K|k)$.

Dimostrazione. Si veda [9], Proposition 1.2.4, Lemma 1.2.6 e Corollary 1.2.7. □

Di seguito, se $L|k$ è un estensione di campi e H è un sottogruppo di $\mathrm{Aut}(L|k)$, indicheremo con L^H il sottocampo intermedio tra L e k dato da $\{\alpha \in L \mid f(\alpha) = \alpha \text{ per ogni } f \in H\}$.

Lemma 2.1.5. *Sia $L|k$ un'estensione di Galois e M un sottocampo intermedio $L \supset M \supset k$. Allora l'estensione $L|M$ è di Galois.*

Dimostrazione. Si veda [3], Chapter 6, Lemma 5.1. □

Teorema 2.1.6 (Corrispondenza di Galois per estensioni di campi finite)**.** *Sia $L|k$ un'estensione di Galois finita e sia $G := \operatorname{Gal}(L|k)$. Allora le mappe*

$$M \mapsto H := \operatorname{Gal}(L|M) \qquad e \qquad H \mapsto M := L^H$$

inducono una biiezione tra i sottocampi intermedi di $L|k$ e i sottogruppi di G che rovescia le inclusioni. L'estensione $M|k$ è di Galois se e solo se H è normale in G e in tal caso si ha $\operatorname{Gal}(M|k) \cong G/H$.

Dimostrazione. Si veda [3], Chapter 6, Theorem 5.4. □

2.2 Estensioni Infinite

Come mostra il seguente Lemma, un'estensione di Galois (infinita) è unione di estensioni di Galois finite.

Lemma 2.2.1. *Sia $K|k$ un estensione di Galois. Allora per ogni estensione intermedia finita $K \supset L \supset k$ esiste un'estensione $K \supset M \supset L$ tale che $M|k$ sia finita e di Galois.*

Dimostrazione. Dato che $L \subset K$ e $K|k$ è separabile per la Proposizione 2.1.4, l'estensione $L|k$ è separabile, quindi per il Teorema 2.1.3 esiste α tale che $L = k(\alpha)$. Sia $M \supset L$ un campo di spezzamento di α su k. Allora $M|k$ è un'estensione finita e di Galois per la Proposizione 2.1.4. □

Proposizione 2.2.2. *Sia $K|k$ un'estensione di Galois e sia $L|k$ un'estensione algebrica con $K \supset L$. Allora ogni k-morfismo $\varphi : L \to K$ si può estendere ad un automorfismo di K.*

Dimostrazione. Si veda [3], Chapter 2, Lemma 1.19. □

Siano $K|k$ è un'estensione di Galois infinita e $K \supset M \supset L \supset k$ campi intermedi, entrambi finiti e di Galois su k. Allora per il Teorema Fondamentale c'è una mappa suriettiva naturale $\operatorname{Gal}(M|k) \to \operatorname{Gal}(L|k) \cong \operatorname{Gal}(M|k)/\operatorname{Gal}(M|L)$ data dal passaggio al quoziente. Indichiamo questa mappa con φ_{LM}. Inoltre, se $K \supset N \supset M$ è un altro campo intermedio, finito e di Galois su k, applicando di nuovo il Teorema Fondamentale si hanno suriezioni naturali $\varphi_{MN} : \operatorname{Gal}(N|k) \to \operatorname{Gal}(M|k) \cong \operatorname{Gal}(N|k)/\operatorname{Gal}(N|M)$ e $\varphi_{LN} : \operatorname{Gal}(N|k) \to \operatorname{Gal}(L|k) \cong \operatorname{Gal}(N|k)/\operatorname{Gal}(N|L)$. Dato che $\operatorname{Gal}(N|M) \subset \operatorname{Gal}(N|L)$, si ha che $\varphi_{LN} = \varphi_{LM} \circ \varphi_{MN}$.

Se denotiamo Λ l'insieme $\{M \subset K \mid M|k \text{ è finita e di Galois}\}$, allora $(\Lambda, \subset)$ è un insieme filtrato: se $M|k$ e $L|k$ sono finite e di Galois, allora anche $ML|k$ lo è, dove ML indica l'intersezione di tutti i campi intermedi che contengono sia M che L ([3], Chapter 6, Lemma 5.1).

Abbiamo quindi che $(\operatorname{Gal}(M|k), \varphi_{ML})_{M\in\Lambda}$ è un sistema inverso di gruppi.

Proposizione 2.2.3. *Con le notazioni precedenti, $\varprojlim_{M\in\Lambda} \operatorname{Gal}(M|k) \cong \operatorname{Gal}(K|k)$.*

Dimostrazione. Definiamo una mappa

$$\begin{aligned} \varphi : \operatorname{Gal}(K|k) &\to \prod_{L\in\Lambda} \operatorname{Gal}(L|k) \\ \sigma &\mapsto (\sigma_{|L})_{L\in\Lambda} \end{aligned}$$

Per Proposizione 2.1.4 questa mappa è ben definita ed è un morfismo di gruppi: $\varphi(\sigma\circ\tau) = ((\sigma\circ\tau)_{|L})_{L\in\Lambda} = (\sigma_{|L} \circ \tau_{|L})_{L\in\Lambda} = (\sigma_{|L})_{L\in\Lambda}(\tau_{|L})_{L\in\Lambda} = \varphi(\sigma)\varphi(\tau)$.

Vediamo che $\operatorname{Im}\varphi = \varprojlim \operatorname{Gal}(M|k)$. Certamente $\varphi(\sigma) = (\sigma_{|L})_{L\in\Lambda}$ è tale che, se $M \supset L$ sono estensioni finite e di Galois su K, allora $\varphi_{LM}(\sigma_{|M}) = (\sigma_{|M})_{|L} = \sigma_{|L}$. Quindi $\operatorname{Im}\varphi \subset \varprojlim \operatorname{Gal}(M|k)$. Per l'altra inclusione, se $(\sigma_L)_{L\in\Lambda} \in \varprojlim \operatorname{Gal}(M|k)$, possiamo definire un automorfismo $\sigma \in \operatorname{Gal}(K|k)$ nel modo seguente. Se $\alpha \in K$, allora per il Lemma 2.2.1 esiste $M \in \Lambda$ tale che $M \supset k(\alpha)$, in particolare $\alpha \in M$. Poniamo $\sigma(\alpha) := \sigma_M(\alpha)$. Allora σ risulta ben definito per la proprietà che definisce $\varprojlim \operatorname{Gal}(M|k)$, e chiaramente $\varphi(\sigma) = (\sigma_L)_{L\in\Lambda}$.

Resta da vedere che φ è iniettiva. Ma questo è vero perché se $\mathrm{id}_K \neq \sigma \in \operatorname{Gal}(K|k)$ allora esiste $\alpha \in K$ tale che $\sigma(\alpha) \neq \alpha$. Sia quindi $M \in \Lambda$ contenente $k(\alpha)$ (Lemma 2.2.1). Allora $\sigma_{|M} \neq \mathrm{id}_M$, quindi $\varphi(\sigma)$ ha almeno una componente non banale e non è l'identità. Abbiamo quindi che φ è iniettiva, da cui $\operatorname{Gal}(K|k) \cong \operatorname{Im}\varphi = \varprojlim \operatorname{Gal}(L|k)$. □

Dotando ognuno dei $\mathrm{Gal}(M|k)$ della topologia discreta possiamo dare a $\mathrm{Gal}(K|k)$ la topologia indotta dal limite, ottenendo un gruppo profinito. D'ora in poi quando parleremo del gruppo di Galois di un'estensione infinita sottointenderemo che sia dotato di questa topologia.

Il prossimo risultato è una generalizzazione del Teorema 2.1.6 per estensioni infinite.

Teorema 2.2.4 (Corrispondenza di Galois per estensioni di campi infinite)**.** *Sia $K|k$ un'estensione di Galois infinita e sia $G := \mathrm{Gal}(K|k)$. Allora le mappe*

$$L \mapsto H := \mathrm{Gal}(K|L) \qquad\qquad e \qquad\qquad H \mapsto L := K^H$$

inducono una biiezione tra sottocampi intermedi di $K|k$ e sottogruppi chiusi di G che rovescia le inclusioni. L'estensione $L|k$ è di Galois se e solo se H è normale in G e in tal caso si ha $\mathrm{Gal}(L|k) \cong G/H$. L'estensione $L|k$ è finita se e solo se H è un sottogruppo aperto di G.

Dimostrazione. Vediamo innanzitutto che se L è un campo intermedio finito su k allora $\mathrm{Gal}(L|k)$ è sia chiuso che aperto in G. Sia $M \supset L$ un'estensione finita e di Galois su k. Allora $\mathrm{Gal}(M|k)$ è uno dei gruppi del sistema inverso che ha come limite G, quindi c'è una suriezione naturale $\pi_M : G \to \mathrm{Gal}(M|k)$ data dalla proiezione sulle componenti. Per il Teorema Fondamentale nel caso finito, $\mathrm{Gal}(M|L)$ è un sottogruppo di $\mathrm{Gal}(M|k)$. Sia $U_L := \pi_M^{-1}(\mathrm{Gal}(M|L))$. Allora U_L è aperto, perché π_M è continua e $\mathrm{Gal}(M|k)$ è discreto. Vediamo che vale $U_L = \mathrm{Gal}(K|L)$. Ogni elemento di U_L è l'identità su L, perché controimmagine di un elemento di $\mathrm{Gal}(M|L)$, quindi vale $U_L \subset \mathrm{Gal}(K|L)$. Per l'altra inclusione si ha che, dato che ogni elemento di $\mathrm{Gal}(K|L)$ è l'identità su L, vale $\pi_M(\mathrm{Gal}(K|L)) \subset \mathrm{Gal}(M|L)$, da cui $\mathrm{Gal}(K|L) \subset \pi_M^{-1}(\pi_M(\mathrm{Gal}(K|L))) \subset \pi_M^{-1}(\mathrm{Gal}(M|L)) = U_L$. Allora per la Proposizione 1.3.4 si ha che $\mathrm{Gal}(K|L)$ è un sottogruppo aperto e chiuso di G.

Sia ora $L|k$ un'estensione arbitraria (non necessariamente finita) contenuta in K. Chiaramente vale $L = \bigcup_{\alpha\in L} k(\alpha)$ e ogni estensione $k(\alpha)|k$ è finita. Ma allora $\mathrm{Gal}(K|L) = \bigcap_{\alpha\in L} \mathrm{Gal}(K|k(\alpha))$ è chiuso, perché come abbiamo visto ognuno dei $\mathrm{Gal}(K|k(\alpha))$ lo è. Dato che K è di Galois su L, si ha $K^{\mathrm{Gal}(K|L)} = L$.

Sia H un sottogruppo chiuso di G e sia $L := K^H$. Allora per definizione $\mathrm{Gal}(K|L) \supset H$. Per l'altra inclusione, supponiamo prima che H sia anche aperto. Allora per il Lemma 1.3.5 si ha che $\ker \pi_M \subset H$ per qualche campo intermedio $K \supset M \supset k$ finito e di Galois su k. Dato che $H \supset \ker \pi_M = \mathrm{Gal}(K|M)$ si ha $L = K^H \subset K^{\ker \pi_M} = M$, quindi $L|k$ è finita. Possiamo quindi applicare il Teorema 2.1.6 ed ottenere $\mathrm{Gal}(K|L) = H$ come richiesto. Si noti che abbiamo anche dimostrato l'ultima parte del Teorema.

Sia ora H chiuso, ma non necessariamente aperto. Per la Proposizione 1.3.4 esiste una famiglia $\mathcal{H}$ di sottogruppi aperti di G con $H = \bigcap \mathcal{H}$. Per ogni $U \in \mathcal{H}$ vale $U \supset H \implies K^U \subset K^H = L \implies \mathrm{Gal}(K|K^U) \supset \mathrm{Gal}(K|L)$. Per quanto visto prima si ha allora $\mathrm{Gal}(K|L) \subset \bigcap_{U\in\mathcal{H}} \mathrm{Gal}(K|K^U) = \bigcap \mathcal{H} = H$.

Sia $L|k$ di Galois e siano $\tau \in H$ e $\sigma \in G$. Dato che per la Proposizione 2.1.4 vale $\sigma(\alpha) \in L$ per ogni $\alpha \in L$, si ha $\tau(\sigma(\alpha)) = \sigma(\alpha)$, quindi $(\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha$, da cui $\sigma^{-1} \circ \tau \circ \sigma \in H$, cioè H è normale in G. Sia ora $H \subset G$ un sottogruppo chiuso e normale e $L = K^H$. Allora, per $\sigma \in G$, $z \in L$ e $\tau \in H$, per normalità di H si ha $(\sigma^{-1} \circ \tau \circ \sigma)(z) = z \implies \tau(\sigma(z)) = \sigma(z) \implies \sigma(z) \in K^H = L$, quindi per la Proposizione 2.1.4 si ha che $L|k$ è di Galois.

Sia ancora $L|k$ di Galois. Per vedere che $\mathrm{Gal}(L|k) \cong G/H$ definiamo una mappa $\psi : G \to \mathrm{Gal}(L|k)$ ponendo $\psi(\sigma) := \sigma_{|L}$. Questa mappa è ben definita per la Proposizione 2.1.4 ed è suriettiva per il Lemma 2.2.2. Il suo nucleo è proprio H: per $\sigma \in G$ si ha $\sigma \in H \iff \sigma(\alpha) = \alpha \,\forall \alpha \in L \iff \sigma_{|L} = \mathrm{id}_L$. □

2.3 Versione di Grothendieck

È possibile riformulare il Teorema 2.2.4 tramite equivalenze di categorie. Fissiamo un campo base k e una sua chiusura algebrica $\overline{k}$.

Definizione 2.3.1. Il campo intermedio $\overline{k} \supset k_s \supset k$ generato da tutte le estensioni finite e separabili di k è detto *chiusura separabile* di k (in $\overline{k}$).

Un campo k è perfetto se e solo se $\overline{k} = k_s$ ([3], Chapter 2, Proposition 2.26). Inoltre $k_s|k$ è un'estensione di Galois ([3], Chapter 2, Proposition 2.16). Il gruppo $\mathrm{Gal}(k) := \mathrm{Gal}(k_s|k)$ è detto *gruppo di Galois assoluto* di k. Grazie alla Proposizione 2.2.3 possiamo considerare $\mathrm{Gal}(k)$ un gruppo topologico profinito.

Siano L un'estensione finita e separabile di k e $\mathrm{Hom}_k(L, k_s)$ l'insieme dei morfismi di k-algebre da L in k_s. Possiamo definire un'azione sinistra di $\mathrm{Gal}(k)$ su $\mathrm{Hom}_k(L, k_s)$ ponendo, per $g \in \mathrm{Gal}(k)$ e $\phi \in \mathrm{Hom}_k(L, k_s)$, $g\phi := g \circ \phi$.

Lemma 2.3.2. *L'azione di* $\mathrm{Gal}(k)$ *su* $\mathrm{Hom}_k(L, k_s)$ *appena definita è continua e transitiva.*

Dimostrazione. Per il Lemma 1.4.4 per avere la continuità basta dimostrare che gli stabilizzatori sono aperti. Ma per $\phi \in \mathrm{Hom}_k(L, k_s)$ si ha $G_\phi = \mathrm{Gal}(k_s|\phi(L))$ e dato che $\phi(L)|k$ è finita questo è aperto per il Teorema 2.2.4. Per la transitività, sia $\alpha \in L$ un elemento primitivo con polinomio minimo $f \in k[x]$. Un elemento $\phi \in \mathrm{Hom}_k(L|k_s)$ è determinato da $\phi(\alpha)$, che è un'altra radice di f. Data una qualunque radice β di f, per la Proposizione 2.2.2 esiste un automorfismo $g \in \mathrm{Gal}(k)$ tale che $g(\phi(\alpha)) = \beta$, quindi $g \circ \phi$ è il morfismo $\psi : L \to k_s$ dato da $\psi(\alpha) = \beta$. Quindi l'azione è transitiva. □

Con le stesse notazioni di prima si ha anche quanto segue.

Lemma 2.3.3. $\mathrm{Hom}_k(L, k_s)$ *è isomorfo all'insieme di classi laterali di un sottogruppo di* $\mathrm{Gal}(k)$ *con azione di* $\mathrm{Gal}(k)$ *per moltiplicazione sinistra. Se* $L|k$ *è di Galois,* $\mathrm{Hom}_k(L, k_s)$ *è isomorfo ad un gruppo quoziente di* $\mathrm{Gal}(k)$ *con azione per moltiplicazione sinistra.*

Dimostrazione. La prima parte deriva direttamente dalla Proposizione 1.4.2. Per la seconda, notiamo che se $L|k$ è di Galois allora per $\phi \in \mathrm{Gal}(k)$ si ha $\phi(L) = L$ per il Lemma 2.2.2. Inoltre per il Teorema 2.2.4 vale $G_\phi = \mathrm{Gal}(k_s|L)$ è normale in $\mathrm{Gal}(k)$, da cui la tesi. □

Se $L|k$ e $M|k$ sono estensioni finite e separabili, allora ogni k-morfismo $\varphi : L \to M$ induce in maniera naturale un morfismo $\mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$ dato da $\sigma \mapsto \sigma \circ \varphi$. Abbiamo quindi un funtore controvariante tra la categoria delle estensioni finite e separabili di k e quella dei $\mathrm{Gal}(k)$-insiemi sinistri finiti con azione continua e transitiva. Tale funtore è un'anti-equivalenza di categorie.

Proposizione 2.3.4. *C'è un'anti-equivalenza tra le categorie delle estensioni finite e separabili di* k *e quella dei* $\mathrm{Gal}(k)$*-insiemi sinistri finiti con azione continua e transitiva. In questa anti-equivalenza, le estensioni di Galois corrispondono ad azioni di* $\mathrm{Gal}(k)$ *su suoi quozienti per moltiplicazione sinistra.*

Dimostrazione. Poniamo per semplicità $G := \mathrm{Gal}(k)$. Per l'essenziale suriettività, sia S un G-insieme sinistro transitivo finito e sia $s \in S$. Allora G_s è un sottogruppo aperto di G per il Lemma 1.4.4, quindi per il Teorema 2.2.4 $L := k_s^{G_s}$ è un'estensione finita e separabile di k. Ma S e $\mathrm{Hom}_k(L, k_s)$ sono entrambi isomorfi all'insieme delle classi laterali di G_s in G per la Proposizione 1.4.2, quindi sono tra loro isomorfi.

Per vedere che il funtore è anche pienamente fedele, sia $f : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$ un morfismo di G-insiemi. Per transitività dell'azione, tale morfismo è determinato dall'immagine di un unico $\phi \in \mathrm{Hom}_k(M, k_s)$; sia $\psi := f(\phi)$. Abbiamo $G_\phi \subset G_\psi$, perché se $g\phi = \phi$ per qualche $g \in G$ allora $g\psi = gf(\phi) = f(g\phi) = f(\phi) = \psi$. Abbiamo quindi $\psi(L) = k_s^{G_\psi} \subset k_s^{G_\phi} = \phi(M)$. Ma allora $\phi^{-1} \circ \psi \in \mathrm{Hom}_k(L, M)$ è l'unico morfismo tra L ed M che induce f e si ha quanto richiesto.

L'ultima affermazione deriva direttamente dal Lemma precedente. □

È possibile rimuovere la condizione di transitività dall'anti-equivalenza descritta, a patto di sostituire le estensioni finite e separabili con le *algebre étale*. Quando parleremo di un algebra A su un campo k assumeremo che il morfismo di algebra $\varphi : k \to A$ sia non nullo (e quindi iniettivo).

Definizione 2.3.5. Una k-algebra finita è detta *étale* se è prodotto diretto di estensioni separabili di k.

Esistono altre definizioni equivalenti di algebra étale, si veda [9], Proposition 1.5.6. Noi utilizzeremo la caratterizzazione data. Notiamo che se $A = \prod_i L_i$ è una k-algebra étale possiamo definire un'azione di $\mathrm{Gal}(k)$ su $\mathrm{Hom}_k(A, k_s)$ esattamente come nel caso delle estensioni separabili.

Grazie al lemma precedente abbiamo che l'azione di $\mathrm{Gal}(k)$ su $\mathrm{Hom}_k(A, k_s)$ è continua: infatti $G_\phi = \mathrm{Gal}(k_s|\phi(\tilde{L}_i))$, dove $\phi : A \to k_s$ è un morfismo di k-algebre e $\tilde{L}_i = L_i \times \prod_{j \neq i}\{0_j\}$ è l'unica componente su cui ϕ è non nullo (se ce ne fosse un'altra $\tilde{L}_j$, dato che $\tilde{L}_i$ e $\tilde{L}_j$ sono campi ϕ sarebbe iniettivo su ognuno di loro e ci sarebbero degli zero-divisori in k_s, assurdo). Inoltre un morfismo di k-algebre $\varphi : A \to B$ induce un morfismo di $\mathrm{Gal}(k)$-insiemi sinistri $\varphi_* : \mathrm{Hom}_k(B, k_s) \to \mathrm{Hom}_k(A, k_s)$. Abbiamo quindi un funtore controvariante tra la categoria delle k-algebre étale e quella dei $\mathrm{Gal}(k)$ insiemi finiti con azione continua.

Teorema 2.3.6 (Corrispondenza di Galois per algebre étale)**.** *Sia* k *un campo. C'è un'anti-equivalenza tra la categoria delle* k*-algebre étale e quella dei* $\mathrm{Gal}(k)$*-insiemi sinistri finiti con azione continua. In questa anti-equivalenza le estensioni separabili corrispondono* $\mathrm{Gal}(k)$*-insiemi con azione transitiva e le estensioni di Galois a* $\mathrm{Gal}(k)$*-insiemi isomorfi a quozienti di* $\mathrm{Gal}(k)$ *con azione per moltiplicazione sinistra.*

Dimostrazione. Se $X = \coprod_{i=1}^{n} \Omega_i$ è un G-insieme sinistro finito con azione continua e Ω_i sono le orbite dell'azione, allora Ω_i è isomorfo a $\mathrm{Hom}_k(L_i, k_s)$ per qualche estensione finita e separabile $L_i|k$ per la Proposizione 2.3.4. Si ha quindi $X = \coprod_{i=1}^{n} \Omega_i \cong \coprod_{i=1}^{n} \mathrm{Hom}_k(L_i, k_s) \cong \mathrm{Hom}_k\left(\prod_{i=1}^{n} L_i, k_s\right)$ per quanto osservato prima, e si ha l'essenziale suriettività.

Il funtore è anche pienamente fedele: se $A = \prod_{i=1}^{n} L_i$ e $B = \prod_{j=1}^{m} M_j$ sono k-algebre étale si ha $\mathrm{Hom}_k(A, B) = \mathrm{Hom}_k(\prod_{i=1}^{n} L_i, \prod_{j=1}^{m} M_j) \cong \coprod_{i,j} \mathrm{Hom}_k(L_i, M_j)$ che per la Proposizione 2.3.4 è in biiezione con l'insieme $\coprod_{i,j} \mathrm{Hom}_G(\mathrm{Hom}_k(M_j, k_s), \mathrm{Hom}_k(L_i, k_s)) \cong \mathrm{Hom}_G(\mathrm{Hom}_k(B, k_s), \mathrm{Hom}_k(A, k_s))$. □

Osservazione 2.3.7. Il Teorema precedente può essere generalizzato ad una qualunque estensione di Galois $K|k$, considerando solo le k-algebre étale che sono prodotto di sottoestensioni di K e i $\mathrm{Gal}(K|k)$-insiemi sinistri finiti con azione continua.

3 Rivestimenti di Spazi Topologici

In questo capitolo studieremo la corrispondenza di Galois per rivestimenti e la riformuleremo poi come equivalenza di categorie, in analogia con quanto fatto nel capitolo precedente. Infine daremo un'altra riformulazione, sempre come equivalenza di categorie, tramite i fasci localmente costanti.

In tutto il capitolo assumeremo per semplicità che tutti gli spazi topologici siano di Hausdorff e che ogni punto ammetta un sistema fondamentale di intorni connessi per archi e semplicemente connessi.

3.1 Rivestimenti, Sollevamenti e Monodromia

Definizione 3.1.1. Siano X, Y spazi topologici e $f : Y \to X$ una mappa continua. Un aperto $U \subset X$ si dice *uniformemente rivestito* se $p^{-1}(U) = \bigcup \mathcal{V}$, dove $\mathcal{V}$ è una famiglia di aperti a due a due disgiunti tali che $f_{|V} : V \to U$ è un omeomorfismo per ogni $V \in \mathcal{V}$.

Definizione 3.1.2. Sia X uno spazio topologico. Uno *spazio su* X è uno spazio topologico Y con una mappa continua $p : Y \to X$. Un *morfismo* tra due spazi $p : Y \to X$ e $q : Z \to X$ su X è una mappa continua $f : Y \to Z$ tale che $q \circ f = p$, cioè che faccia commutare il diagramma

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[dr, "p"'] & Z \arrow[d, "q"] \\ & X \end{tikzcd}$$

Indicheremo con $\mathrm{Hom}_X(Y, Z)$ l'insieme dei morfismi come spazi su X tra Y e Z. Uno spazio Y su X si dice *rivestimento* se la mappa $p : Y \to X$ è suriettiva e tale che ogni punto di X abbia un intorno uniformemente rivestito. Diciamo che un rivestimento $p : Y \to X$ è *connesso* e Y lo è.

Osservazione 3.1.3. Sia $p : Y \to X$ un rivestimento. Allora le fibre $p^{-1}(x)$, al variare di x, sono sottospazi discreti di Y e, se X è connesso, hanno tutte la stessa cardinalità ([9], Corollary 2.1.4). Ha quindi senso chiamare *finito* un rivestimento $p : Y \to X$ se le fibre $p^{-1}(x)$ lo sono.

Proposizione 3.1.4. *Sia $p : Y \to X$ un rivestimento. Allora p è una mappa aperta e X ha la topologia quoziente rispetto a p.*

Dimostrazione. Si veda [4], Theorem 17.3. □

Definizione 3.1.5. Sia $p : Y \to X$ un rivestimento e sia $f : Z \to X$ una mappa continua. Una mappa continua $\tilde{f} : Z \to Y$ tale che $p \circ \tilde{f} = f$, cioè che faccia commutare il diagramma

$$\begin{tikzcd} & Y \arrow[d, "p"] \\ Z \arrow[ur, "\tilde{f}"] \arrow[r, "f"] & X \end{tikzcd} \tag{4}$$

è detta *sollevamento* di f.

Non tutte le funzioni continue ammettono sollevamenti, ma se il dominio è connesso, sollevamenti con un punto in comune coincidono. Vale un risultato più generale.

Lemma 3.1.6. *Siano $p : Y \to X$ un rivestimento, Z uno spazio connesso e $f, g : Z \to Y$ due mappe continue tali che $p \circ f = p \circ g$. Se per qualche $z \in Z$ si ha $f(z) = g(z)$, allora $f = g$.*

Dimostrazione. Si veda [9], Proposition 2.2.2 oppure [4], Lemma 17.4. □

Come semplice corollario abbiamo quanto detto prima.

Proposizione 3.1.7. *Siano $p : Y \to X$ un rivestimento, Z connesso e $f : Z \to X$ una mappa continua. Se $f_1, f_2 : Z \to Y$ sono due sollevamenti di f e $f_1(z) = f_2(z)$ per qualche $z \in Z$, allora $f_1 = f_2$.*

Nei casi particolari di archi e omotopie è assicurata anche l'esistenza dei sollevamenti, per ogni scelta coerente del punto iniziale.

Teorema 3.1.8. *Sia $p : Y \to X$ un rivestimento.*

(1) Siano $f : [0, 1] \to X$ un arco in X e $y \in Y$ tale che $p(y) = f(0)$. Allora esiste un unico sollevamento $\tilde{f} : [0, 1] \to Y$ di f tale che $\tilde{f}(0) = y$.

(2) Siano Z uno spazio topologico e $f : Z \to X$ una mappa continua che ammette un sollevamento $\tilde{f} : Z \to Y$. Sia $F : Z \times [0, 1] \to X$ una mappa continua tale che $F(z, 0) = f(z)\, \forall z \in Z$. Allora esiste un unico sollevamento $\tilde{F} : Z \times [0, 1] \to Y$ di F tale che $\tilde{F}(z, 0) = \tilde{f}(z)\, \forall z \in Z$.

Dimostrazione. Si veda [2] Part I, (5.3) e (5.4) oppure [4], Theorem 17.6. □

D'ora in avanti, se $p : Y \to X$ è un rivestimento, α un arco in X e $y \in p^{-1}(\alpha(0))$, indicheremo con $l_y(\alpha)$ l'unico sollevamento di α con punto iniziale y. Il seguente Corollario è immediato.

Corollario 3.1.9 (Monodromia)**.** *Sia $p : Y \to X$ un rivestimento. Se α, β sono due archi equivalenti in X (cioè omotopi relativamente a $\{0, 1\}$) di punto iniziale x e $y \in p^{-1}(x)$, allora $l_y(\alpha)$ e $l_y(\beta)$ sono archi equivalenti in Y, in particolare $l_y(\alpha)(1) = l_y(\beta)(1)$.*

3.2 Automorfismi di Rivestimenti

Notiamo che, fissato uno spazio topologico X, gli spazi su X con i relativi morfismi formano una categoria. Se stabiliamo che i *morfismi di rivestimenti* sono semplicemente i morfismi di spazi su X tra due rivestimenti, abbiamo che i rivestimenti di X sono una sottocategoria piena degli spazi su X. Dato un rivestimento $p : Y \to X$, denotiamo con $\mathrm{Aut}(Y|X)$ il suo gruppo di automorfismi.

Lemma 3.2.1. *Siano $p : Y \to X$ un rivestimento connesso e $\varphi \in \mathrm{Aut}(Y|X)$. Se φ ha un punto fisso, allora è l'identità.*

Dimostrazione. Dal Lemma 3.1.6, ponendo $Z = Y$, $f = \mathrm{id}$ e $g = \varphi$. □

Proposizione 3.2.2. *Sia X un G-spazio. Se l'azione di G è propriamente discontinua, la proiezione canonica $p : X \to X/G$ è un rivestimento. Inoltre se X è connesso vale $\mathrm{Aut}(X|X/G) \cong G$. Infine, se H è un sottogruppo normale di G, allora X/H è un G/H-spazio e vale $(X/H)/(G/H) \cong X/G$*

Dimostrazione. Si veda [9] Proposition 2.2.3 e Proposition 2.2.4. □

Se $p : Y \to X$ è un rivestimento connesso e $H = \mathrm{Aut}(Y|X)$, l'azione naturale di H su Y è propriamente discontinua ([4], Theorem 21.8). C'è quindi un rivestimento $p' : Y \to Y/H$. Non è però sempre vero che $Y/H \cong X$. Tuttavia dalla definizione di morfismo di rivestimenti e dal fatto che p' è aperta si ha che esiste un'unica mappa continua $q : Y/H \to X$ che faccia commutare il seguente diagramma

$$\begin{tikzcd} Y \arrow[r, "p'"] \arrow[dr, "p"'] & Y/H \arrow[d, "q"] \\ & X \end{tikzcd} \tag{5}$$

Possiamo quindi dare la seguente definizione, in analogia con il caso delle estensioni di campi.

Definizione 3.2.3. Un rivestimento connesso $p : Y \to X$ è detto *di Galois* se la mappa q nel diagramma (5) è un omeomorfismo, cioè se $Y/\operatorname{Aut}(Y|X) \cong X$.

Osservazione 3.2.4. Se X è un G-spazio e l'azione di G è propriamente discontinua, il rivestimento $p : X \to X/G$ è di Galois.

Proposizione 3.2.5. *Un rivestimento connesso $p : Y \to X$ è di Galois se e solo se l'azione naturale di $H = \operatorname{Aut}(Y|X)$ su ciascuna fibra è transitiva.*

Dimostrazione. Se il rivestimento è di Galois, la mappa $q : Y/H \to X$ del diagramma (5) è biiettiva. Quindi la fibra di un qualunque $x \in X$ viene mappata in un solo elemento di Y/H, cioè l'azione di H su $p^{-1}(x)$ è transitiva. Viceversa, se l'azione è transitiva la mappa continua q deve essere biiettiva. È anche aperta, perché lo sono $p : Y \to X$ e la mappa di passaggio al quoziente $Y \to Y/H$ sono sia aperte che continue. Quindi q è un omeomorfismo e il rivestimento $p : Y \to X$ è di Galois. □

Lemma 3.2.6. *Siano $q : Z \to X$ un rivestimento connesso e $f : Y \to Z$ una mappa continua. Se $q \circ f : Y \to X$ è un rivestimento, allora anche $f : Y \to Z$ lo è.*

Dimostrazione. Si veda [9], Lemma 2.2.11. □

Possiamo ora provare un risultato analogo ai Teoremi 2.1.6 e 2.2.4.

Teorema 3.2.7 (Corrispondenza di Galois per rivestimenti)**.** *Sia $p : Y \to X$ un rivestimento di Galois. Poniamo $G := \operatorname{Aut}(Y|X)$. Per ogni sottogruppo H di G, detta $p_H : Y \to Y/H$ la proiezione canonica, c'è una mappa naturale $\overline{p}_H : Y/H \to X$ che fa commutare il diagramma*

$$\begin{tikzcd} Y \arrow[r, "p_H"] \arrow[dr, "p"'] & Y/H \arrow[d, "\overline{p}_H"] \\ & X \end{tikzcd}$$

Inoltre $\overline{p}_H : Y/H \to X$ è un rivestimento.

Viceversa, dati un rivestimento connesso $q : Z \to X$ e una mappa continua $f : Y \to Z$ che faccia commutare il diagramma

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[dr, "p"'] & Z \arrow[d, "q"] \\ & X \end{tikzcd}$$

si ha che $f : Y \to Z$ è un rivestimento di Galois e posto $H := \operatorname{Aut}(Y|Z)$ si ha $Z \cong Y/H$.

Il rivestimento $q : Z \to X$ è di Galois se e solo se H è normale in G e in tal caso $\operatorname{Aut}(Z|X) \cong G/H$.

Dimostrazione. Sia H un sottogruppo di G. Per la definizione di morfismo di rivestimenti e dal fatto che p_H è aperta si ha che esiste un'unica mappa continua $\overline{p}_H$ tale che $\overline{p}_H \circ p_H = p$. Inoltre $\overline{p}_H$ è suriettiva, perché p lo è. Siano ora $x \in X$ e V un intorno di x uniformemente rivestito da una famiglia $\mathcal{V}$ tale che $\bigcup \mathcal{V} = p^{-1}(V)$. Per $U \in \mathcal{V}$, dato che $P_{|U}$ è un omeomorfismo, $p_{H|U}$ deve essere iniettiva e quindi, dato che è aperta, un omeomorfismo sulla sua immagine. Allora $\{p_H(U) \mid U \in \mathcal{V}\}$ è una famiglia di aperti di Y/H che riveste uniformemente V. Quindi $\overline{p}_H : Y/H \to X$ è un rivestimento.

Viceversa siano $q : Z \to X$ un rivestimento e $f : Y \to Z$ una mappa continua tale che $q \circ f = p$. Allora per il Lemma 3.2.6 $f : Y \to Z$ è un rivestimento, da cui si ha immediatamente che $H = \operatorname{Aut}(Y|Z)$ è un sottogruppo di G. Per vedere che $f : Y \to Z$ è di Galois, grazie alla Proposizione 3.2.5 basta dimostrare che l'azione di H su ciascuna fibra di f è transitiva. Sia quindi $z \in Z$ e siano $y_1, y_2 \in f^{-1}(z) \subset p^{-1}(q(z))$. Dato che $p : Y \to X$ è di Galois esiste un $\varphi \in G$ tale che $\varphi(y_1) = y_2$. Per vedere che $\varphi \in H$ basta mostrare che $f \circ \varphi = f$; ma questo deriva dalla Proposizione 3.1.6, scambiando i ruoli di Y e Z e ponendo $p = q$ e $g = f \circ \varphi$. Per definizione di rivestimento di Galois si ha $Z \cong Y/H$.

Per l'ultima parte, se H è normale in G allora $Z/(G/H) = (Y/H)/(G/H) \cong Y/G \cong X$ per la Proposizione 3.2.2, da cui si ha che $\operatorname{Aut}(Z|X) \cong G/H$ e che $q : Z \to X$ è di Galois. Viceversa, sia $q : Z \to X$ di Galois. Vediamo che per ogni $\varphi \in \operatorname{Aut}(Y|X)$ esiste un unico $\psi_\varphi \in \operatorname{Aut}(Z|X)$ tale che $f \circ \varphi = \psi_\varphi \circ f$. Per $y \in Y$ i punti $f(y)$ e $f(\varphi(y))$ sono nella stessa fibra di q e dato che $q : Z \to X$ è di Galois l'azione di $\mathrm{Aut}(Z|X)$ su tale fibra è transitiva, quindi esiste $\rho \in \mathrm{Aut}(Z|X)$ tale che $\rho(f(y)) = f(\varphi(y))$. Ma per il Lemma 3.2.1 tale ρ è unico e per la Proposizione 3.1.6 vale $\rho \circ f = f \circ \varphi$. Poniamo quindi $\psi_\varphi := \rho$. Definiamo una mappa $m : G \to \mathrm{Aut}(Z|X)$ ponendo $m(\varphi) := \psi_\varphi$. Si verifica facilmente che m è un morfismo di gruppi il cui nucleo è proprio H, che è quindi normale in G. □

3.3 Rivestimenti Universali

Fissiamo da qui in avanti uno spazio topologico connesso X che soddisfi le ipotesi di inizio capitolo; fissiamo inoltre un punto $x \in X$. Ricordiamo che il gruppo fondamentale $\pi_1(X, x)$ di X rispetto al punto x è l'insieme delle classi di equivalenza di lacci di punto base x con l'operazione $[\alpha][\beta] := [\alpha * \beta]$, dove

$$(\alpha * \beta)(t) := \begin{cases} \beta(2t) & \text{se} \quad 0 \le t < \frac{1}{2} \\ \alpha(2t-1) & \text{se} \quad \frac{1}{2} \le t < 1 \end{cases}$$

Tale regola di composizione è in analogia con la composizione di funzioni, ma in contrasto con l'usuale composizione di archi. C'è un isomorfismo canonico dato da $g \mapsto g^{-1}$ tra il gruppo fondamentale definito in questo modo e quello definito con la composizione classica.

Vogliamo ora dare un analogo del Teorema 2.3.6 nel caso dei rivestimenti. Per farlo, abbiamo bisogno di un rivestimento che giochi il ruolo della chiusura separabile di un campo.

Definizione 3.3.1. Un rivestimento connesso $\pi : \tilde{X} \to X$ è detto *universale* se per ogni rivestimento connesso $p : Y \to X$ e punti $\tilde{x} \in \pi^{-1}(x)$ e $y \in p^{-1}(x)$ esiste un unico morfismo di rivestimenti $q : \tilde{X} \to Y$ tale che $q(\tilde{x}) = y$.

Ogni spazio connesso, localmente connesso per archi e semilocalmente semplicemente connesso (in particolare anche il nostro spazio base X) ammette un rivestimento universale ([4], Theorem 22.1). Inoltre un rivestimento $\pi : \tilde{X} \to X$ è universale se e solo se $\tilde{X}$ è semplicemente connesso ([9], Proposition 2.4.9 e Lemma 2.4.10). Nel seguito in molte dimostrazioni useremo solo la proprietà universale e non altre caratterizzazioni. In analogia con il caso algebrico abbiamo quanto segue.

Proposizione 3.3.2. *Un rivestimento universale $\pi : \tilde{X} \to X$ è di Galois.*

Dimostrazione. Per la Proposizione 3.2.5 basta dimostrare che l'azione di $\mathrm{Aut}(\tilde{X}|X)$ su $\pi^{-1}(x)$ è transitiva. Sia quindi $\tilde{y} \in \pi^{-1}(x)$. Per la proprietà universale esistono morfismi $p, q : \tilde{X} \to \tilde{X}$ con $p(\tilde{x}) = \tilde{y}$ e $q(\tilde{y}) = \tilde{x}$. Ma allora $(p \circ q)(\tilde{y}) = \tilde{y}$, quindi $p \circ q = \mathrm{id}_{\tilde{X}}$ per il Lemma 3.2.1. Allora in particolare $p \in \mathrm{Aut}(\tilde{X}|X)$ e $p(\tilde{x}) = \tilde{y}$, come richiesto. □

Fissiamo per il resto del paragrafo anche un rivestimento universale $\pi : \tilde{X} \to X$ e un punto $\tilde{x} \in \pi^{-1}(x)$.

Notiamo che, grazie alla proprietà universale che definisce $\pi : \tilde{X} \to X$, dato un rivestimento $p : Y \to X$ abbiamo una biiezione $\Psi : p^{-1}(x) \to \mathrm{Hom}_X(\tilde{X}, Y)$ che manda un punto $y \in p^{-1}(x)$ nell'unico morfismo $\pi_y : \tilde{X} \to Y$ con $\pi_y(\tilde{x}) = y$. Abbiamo inoltre un'azione *destra* naturale di $\mathrm{Aut}(\tilde{X}|X)$ su $\mathrm{Hom}_X(\tilde{X}, Y)$ data dalla composizione a destra. Possiamo trasformarla in un'azione sinistra componendo a destra per l'inversa: per $\varphi \in \mathrm{Aut}(\tilde{X}|X)$ e $f \in \mathrm{Hom}_X(\tilde{X}, Y)$ poniamo $\varphi f := f \circ \varphi^{-1}$.

Definiamo ora un'azione sinistra di $\pi_1(X, x)$ su $p^{-1}(x)$ ponendo, per $[\alpha] \in \pi_1(X, x)$ e $y \in p^{-1}(x)$, $[\alpha]y := l_y(\alpha)(1)$. Quest'azione è detta *azione di monodromia* ed è ben definita grazie al Corollario 3.1.9.

Proposizione 3.3.3. *C'è un isomorfismo di gruppi $\Phi : \pi_1(X, x) \to \mathrm{Aut}(\tilde{X}|X)$. Inoltre, dato un qualunque rivestimento $p : Y \to X$, l'azione di $\mathrm{Aut}(\tilde{X}|X)$ su $\mathrm{Hom}_X(\tilde{X}, Y)$ è esattamente l'azione di monodromia di $\pi_1(X, x)$ su $p^{-1}(x)$, cioè per $[\alpha] \in \pi_1(X, x)$ e $y \in p^{-1}(x)$ vale $\Psi([\alpha]y) = \Phi([\alpha])\Psi(y)$.*

Dimostrazione. Sia $\alpha : [0, 1] \to X$ un laccio in X di punto base x. Dato che l'azione di $\mathrm{Aut}(\tilde{X}|X)$ su $\pi^{-1}(x)$ è transitiva (Proposizione 3.3.2), si ha che esiste un $g_\alpha \in \mathrm{Aut}(\tilde{X}|X)$ tale che $g_\alpha(\tilde{x}) = l_{\tilde{x}}(\alpha)(1)$. Inoltre tale g_α è unico per la proprietà universale e non dipende dalla classe di α in $\pi_1(X, x)$ per il Corollario 3.1.9. Definiamo una mappa $\Phi : \pi_1(X, x) \to \mathrm{Aut}(\tilde{X}|X)$ ponendo $\Phi([\alpha]) := g_\alpha^{-1}$. Questa mappa è un morfismo di gruppi: per $[\alpha], [\beta] \in \pi_1(X, x)$, posto $\tilde{x}' := l_{\tilde{x}}(\beta)(1)$, si ha che $\Phi([\alpha][\beta]) = g_{\alpha * \beta}$ è l'unico elemento di $\mathrm{Aut}(\tilde{X}|X)$ tale che $g_{\alpha*\beta}(\tilde{x}) = l_{\tilde{x}}(\alpha * \beta)(1) = l_{\tilde{x}'}(\alpha)(1)$. Ma $a(t) := g_\beta(l_{\tilde{x}}(\alpha)(t))$ è un sollevamento di α che inizia in $\tilde{x}'$, quindi coincide con $l_{\tilde{x}'}(\alpha)$ e si ha $g_{\alpha*\beta}(\tilde{x}) = a(1) = g_\beta(l_{\tilde{x}}(\alpha)(1)) = (g_\beta \circ g_\alpha)(\tilde{x})$, quindi $\Phi([\alpha][\beta]) = (g_\beta \circ g_\alpha)^{-1} = \Phi([\alpha])\Phi([\beta])$. È anche una biiezione, perché un automorfismo

$g : \tilde{X} \to \tilde{X}$ è dato da $\Phi([\pi \circ \alpha])$, dove $\alpha : [0,1] \to \tilde{X}$ è un arco da $\tilde{x}$ a $g(\tilde{x})$: due tali archi α e β sono equivalenti perché $\tilde{X}$ è semplicemente connesso, quindi $[\pi \circ \alpha] = [\pi \circ \beta]$ in $\pi_1(X,x)$.

Per la seconda parte si ha che, per $[\alpha] \in \pi_1(X,x)$ e $y \in p^{-1}(x)$ e posto $\pi_y = \Psi(y)$, vale $\Psi([\alpha]y) = \Psi(l_y(\alpha)(1)) = \Psi(\pi_y(l_{\tilde{x}}(\alpha)(1))) = \Psi(\pi_y(g_\alpha(\tilde{x}))) = \Psi((\Phi([\alpha])\pi_y)(\tilde{x})) = \Phi([\alpha])\Psi(y)$. □

Definiamo quindi un funtore covariante Fib_x dalla categoria dei rivestimenti di X a quella dei $\pi_1(X,x)$-insiemi sinistri nel modo seguente. Un rivestimento $p : Y \to X$ viene mandato nella fibra $\mathrm{Fib}_x(p : Y \to X) := \pi^{-1}(x)$ equipaggiata con l'azione di monodromia su Y e un morfismo di rivestimenti $f : Y \to Z$ nella sua restrizione alla fibra $\mathrm{Fib}_x(f) := f_{|p^{-1}(x)}$. Si noti che per definizione di morfismo la mappa $\mathrm{Fib}_x(f)$ è ben definita. È inoltre un morfismo di $\pi_1(X,x)$-insiemi: se $[\alpha] \in \pi_1(X,x)$ e $y \in p^{-1}(x)$ si ha $\mathrm{Fib}_x(f)([\alpha]y) = \mathrm{Fib}_x(f)(l_y(\alpha)(1)) = l_{f(y)}(\alpha)(1) = [\alpha]\,\mathrm{Fib}_x(f)(y)$ per l'unicità del sollevamento.

Teorema 3.3.4. *C'è un'equivalenza tra la categoria dei rivestimenti di X e quella dei $\pi_1(X,x)$-insiemi sinistri. In questa equivalenza, i rivestimenti connessi corrispondono a $\pi_1(X,x)$-insiemi con azione transitiva e i rivestimenti di Galois a $\pi_1(X,x)$-insiemi isomorfi a quozienti di $\pi_1(X,x)$ con azione per moltiplicazione sinistra.*

Dimostrazione. Poniamo per semplicità $G := \pi_1(X,x)$. Per l'essenziale suriettività, sia S un G-insieme sinistro e sia $s \in S$ e assumiamo dapprima che l'azione di G su S sia transitiva. Sia allora $G_s \leq G$ lo stabilizzatore di s e sia $Y := \tilde{X}/\Phi(G_s)$ il rivestimento connesso $p : Y \to X$ di cui il Teorema 3.2.7 assicura l'esistenza. Ma allora S e $p^{-1}(x)$ sono isomorfi come G-insiemi per la Proposizione 1.4.2. Viceversa, se prendiamo Y connesso l'azione di G su $p^{-1}(x)$ è certamente transitiva, perché lo è su $\pi^{-1}(x)$ e $p^{-1}(x)$ è un suo quoziente per il Teorema 3.2.7. Se il rivestimento $p : Y \to X$ è inoltre di Galois, abbiamo che lo stabilizzatore H di un qualunque punto di $p^{-1}(x)$ è normale in G, quindi l'azione di G su G/H, isomorfa all'azione di G su $p^{-1}(x)$, diventa un'azione per moltiplicazione sinistra su un quoziente.

Se l'azione di G su S non è transitiva, è sufficiente decomporlo nell'unione disgiunta delle sue orbite $S = \coprod_i \Omega_i$, trovare per ogni orbita un rivestimento $p_i : Y_i \to X$ e prendere l'unione disgiunta $\coprod_i Y_i$ di questi rivestimenti, che è ancora un rivestimento (questa volta non connesso) di X.

Per vedere che il funtore è anche pienamente fedele, siano $p : Y \to X$ e $q : Z \to X$ due rivestimenti e sia $f : p^{-1}(x) \to q^{-1}(x)$ un morfismo di G-insiemi sinistri. Supponiamo dapprima che Y e Z siano connessi, e quindi le azioni di G su $p^{-1}(x)$ e $q^{-1}(x)$ transitive. Fissiamo $y \in p^{-1}(x)$ e sia $z = f(y)$. Siano $\pi_y : \tilde{X} \to Y$ e $\pi_z : \tilde{X} \to Z$ i morfismi di rivestimenti con $\pi_y(\tilde{x}) = y$ e $\pi_z(\tilde{x}) = z$ dati dalla proprietà universale. Per il Teorema 3.2.7 esistono rivestimenti $\tilde{p} : \tilde{X}/\operatorname{Aut}(\tilde{X}|Y) \to X$ e $\tilde{q} : \tilde{X}/\operatorname{Aut}(\tilde{X}|Z) \to X$ e isomorfismi di rivestimenti $\varphi : \tilde{X}/\operatorname{Aut}(\tilde{X}|Y) \to Y$ e $\psi : \tilde{X}/\operatorname{Aut}(\tilde{X}|Z) \to Z$. Dette $\rho_y : \tilde{X} \to \tilde{X}/\operatorname{Aut}(\tilde{X}|Y)$ e $\rho_z : \tilde{X} \to \tilde{X}/\operatorname{Aut}(\tilde{X}|Z)$ le mappe di passaggio al quoziente si ha $\pi_y = \varphi \circ \rho_y$ e $\pi_z = \psi \circ \rho_z$. Ma $\operatorname{Aut}(\tilde{X}|Y)$ corrisponde allo stabilizzatore G_y di y in G (e $\operatorname{Aut}(\tilde{X}|Z)$ a G_z). Vale $G_y \subset G_z$: se $g \in G_y$ allora $gz = gf(y) = f(gy) = f(y) = z$, quindi $g \in G_z$. Quindi vale $\operatorname{Aut}(\tilde{X}|Y) \subset \operatorname{Aut}(\tilde{X}|Z)$ e si ha che la mappa ρ_z passa al quoziente rispetto a ρ_y. Esiste quindi un'unica mappa continua $g : \tilde{X}/\operatorname{Aut}(\tilde{X}|Y) \to \tilde{X}/\operatorname{Aut}(\tilde{X}|Z)$ tale che $\rho_z = g \circ \rho_y$, che è quindi un morfismo di rivestimenti. Vale inoltre $g(\varphi^{-1}(y)) = g(\rho_y(\tilde{x})) = \rho_z(\tilde{x}) = \psi^{-1}(z)$, quindi $\psi \circ g \circ \varphi^{-1} : Y \to Z$ è l'unico morfismo di rivestimenti tale che $\mathrm{Fib}_x(\psi \circ g \circ \varphi^{-1}) = f$.

Infine, se Y e Z non sono connessi, si decompongono nelle unioni disgiunte delle loro componenti connesse $Y = \coprod_i Y_i$ e $Z = \coprod_j Z_j$. Ogni componente Y_i e Z_j è a sua volta un rivestimento di X tramite le mappe $p_i := p_{|Y_i}$ e $q_j := q_{|Z_j}$. In questo modo i G-insiemi $p^{-1}(x)$ e $q^{-1}(x)$ si decompongono nelle orbite $p^{-1}(x) = \coprod_i p_i^{-1}(x)$ e $q^{-1}(x) = \coprod_j q_j^{-1}(x)$. Un morfismo di G-insiemi $f : p^{-1}(x) \to q^{-1}(x)$ è dato quindi dall'unione dei morfismi $f_i := f_{|p_i^{-1}(x)}$. Ma l'immagine di un f_i è tutta contenuta nella stessa orbita $q_j^{-1}(x)$: per $g \in G$ e $y \in p_i^{-1}(x)$ vale $f(gy) = gf(y)$, quindi $f(gy)$ è nella stessa orbita di $f(y)$. Grazie a quanto visto prima possiamo quindi dare una famiglia di morfismi di rivestimenti $\{g_i : Y_i \to Z_j\}$ tali che $\mathrm{Fib}_x(g_i) = f_i$ e concludere che $g = \bigcup_i g_i$ è l'unico morfismo $g : Y \to Z$ tale che $f = \bigcup_i f_i = \mathrm{Fib}_x(g)$. □

Il seguente Corollario è ancora più simile al Teorema 2.3.6. Rimandiamo a [9], Corollary 2.3.9 per la dimostrazione.

Corollario 3.3.5. *C'è un'equivalenza tra la categoria dei rivestimenti finiti di X e quella dei $\widehat{\pi_1(X,x)}$-insiemi sinistri finiti con azione di $\widehat{\pi_1(X,x)}$ continua. In questa equivalenza, i rivestimenti connessi corrispondono a $\widehat{\pi_1(X,x)}$-insiemi con azione transitiva e i rivestimenti di Galois a $\widehat{\pi_1(X,x)}$-insiemi isomorfi a quozienti di $\widehat{\pi_1(X,x)}$ rispetto a sottogruppi aperti normali con azione per moltiplicazione sinistra.*

3.4 Riformulazione Tramite Fasci Localmente Costanti

Ricordiamo che dati spazi topologici A, B e $C \subset B$ e una mappa continua $f : A \to B$, una *sezione* di f su C è una mappa continua $g : C \to A$ tale che $f \circ g = \mathrm{id}_C$.

Dato uno spazio $p : Y \to X$ su X, definiamo un prefascio $\mathcal{F}_Y$ su X ponendo, per $U \subset X$ aperto, $\mathcal{F}_Y(U) := \{f : U \to Y \mid f \text{ è una sezione di } p\}$. Per $V \subset U$ le mappe di restrizione $\mathcal{F}_Y(U) \to \mathcal{F}_Y(V)$ sono proprio le restrizioni da U a V. Si noti che $\mathcal{F}_Y$ è anche un fascio, perché le mappe continue soddisfano gli assiomi 1 e 2 della Definizione 1.5.1. Si noti inoltre che se $p : Y \to X$ è un rivestimento, preso un intorno connesso e uniformemente rivestito V di un qualunque $x \in X$, si ha che la restrizione di $\mathcal{F}_Y$ a V è costante. Infatti, una sezione di p su V è un omeomorfismo su una delle componenti connesse W di $p^{-1}(V)$, quindi è l'inverso di $p_{|W}$. Quindi $\mathcal{F}_Y(U)$ è in biiezione canonica con $\{f : V \to p^{-1}(x) \mid f \text{ continua}\}$ per ogni $U \subset V$, cioè $\mathcal{F}_Y$ ristretto a V è un fascio costante. Quindi, se $p : Y \to X$ è un rivestimento, $\mathcal{F}_Y$ è localmente costante.

Dato un altro rivestimento $q : Z \to X$ e un morfismo di rivestimenti $f : Y \to Z$, possiamo definire una morfismo di fasci $\mathcal{F}_Y \to \mathcal{F}_Z$ mandando una sezione $s : U \to Y$ in $f \circ s$. Questa è effettivamente una sezione di q: se prendiamo un ricoprimento U formato da insiemi U_i connessi e uniformemente rivestiti sia da p che da q abbiamo che $(f \circ s)_{|U_i}$ è una sezione di q su U_i per ogni i. Quindi $f \circ s$ è una sezione di q su U per il secondo assioma della definizione di fascio. Abbiamo allora un funtore $S : Y \mapsto \mathcal{F}_Y$ dalla categoria dei rivestimenti su X a quella dei fasci localmente costanti su X (quest'ultima è una sottocategoria piena dei prefasci su X).

Viceversa, ad un fascio localmente costante $\mathcal{F}$ su X possiamo associare un rivestimento $p_\mathcal{F} : X_\mathcal{F} \to X$. Poniamo $X_\mathcal{F} := \coprod_{x \in X} \mathcal{F}_x$ e definiamo $p_\mathcal{F}$ ponendo $p_\mathcal{F}([s]) := x$ se $[s] \in \mathcal{F}_x$. Si noti che $p_\mathcal{F}$ è suriettiva. Per ogni $U \subset X$ aperto e ogni $s \in \mathcal{F}(U)$ per la costruzione dell'Esempio 1.2.5 è ben definita una mappa $i_s : U \to X_\mathcal{F}$ data da $i_s(u) := [s] \in \mathcal{F}_u$. Diamo ad $X_\mathcal{F}$ la topologia generata dalla famiglia $\{i_s(U) \mid U \subset X \text{ aperto}, s \in \mathcal{F}(U)\} \subset 2^{X_\mathcal{F}}$. Si ha che $p_\mathcal{F}$ è continua rispetto a questa topologia: se $U \subset X$ è aperto allora lo è anche $p_\mathcal{F}^{-1}(U) = \coprod_{u \in U} \mathcal{F}_u = \bigcup_{s \in \mathcal{F}(U)} i_s(U)$. È anche un rivestimento: sia $U \subset X$ un intorno aperto connesso di x tale che $\mathcal{F}$ ristretto ad U sia il fascio costante $\mathcal{F}_S$, per S spazio discreto. Allora $p_\mathcal{F}^{-1}(U) = \bigcup_{s \in \mathcal{F}(U)} i_s(U)$ e $p_{\mathcal{F}|i_s(U)}$ è un omeomorfismo (la sua inversa è proprio i_s, che è continua). Inoltre $i_s(U) \cap i_t(U) = \emptyset$ per $s \neq t$: altrimenti esisterebbe $u \in U$ tale che $[s] = [t]$ in $\mathcal{F}_u$, in particolare $s(u) = t(u)$, ma s e t sono costati e si avrebbe $s = t$ su U. Quindi U è uniformemente rivestito.

Dato un morfismo $\phi : \mathcal{F} \to \mathcal{G}$ di fasci localmente costanti su X abbiamo una mappa indotta $\Phi : X_\mathcal{F} \to X_\mathcal{G}$ definita da $\Phi := \coprod_{x \in X} \phi_x$, dove $\phi_x : \mathcal{F}_x \to \mathcal{G}_x$ è il morfismo indotto sulle spighe. La mappa Φ è chiaramente compatibile con $p_\mathcal{F}$ e $p_\mathcal{G}$, cioè $p_\mathcal{F} = p_\mathcal{G} \circ \Phi$. Inoltre è continua: per verificarlo sia $i_t(U) \subset X_\mathcal{G}$ con U aperto in X e $t \in \mathcal{G}(U)$ e siano $[s] \in \Phi^{-1}(i_t(U))$ e $x \in X$ tale che $[s] \in \mathcal{F}_x$. Dato che $\Phi([s]) = \phi_x([s]) = [t] \in \mathcal{G}_x$ abbiamo $x \in U$, possiamo scegliere $V \subset U$ aperto tale che $\phi_V(s_{|V}) = t_{|V}$. Si ha quindi che $i_s(V) \subset X_\mathcal{F}$ è un intorno aperto di $[s] = [s_{|V}]$ contenuto in $\Phi^{-1}(i_t(U))$, che è quindi aperto. Abbiamo allora che $R : \mathcal{F} \mapsto X_\mathcal{F}$ è un funtore, che assieme ad S dà un equivalenza di categorie.

Teorema 3.4.1. *C'è un'equivalenza tra le categorie dei rivestimenti di X e quella dei fasci localmente costanti su X.*

Dimostrazione. Verifichiamo che i funtori S ed R soddisfano la condizione del Lemma 1.1.6. Siano C la categoria dei rivestimenti di X e D la categoria dei fasci localmente costanti su X. Per dare un isomorfismo $\Phi : R \circ S \to \mathrm{id}_C$ dobbiamo trovare, per ogni $Y, Z \in C$, isomorfismi $\Phi_Y : X_{\mathcal{F}_Y} \to Y$ e $\Phi_Z : X_{\mathcal{F}_Z} \to Z$ tali che, per ogni $f \in \mathrm{Hom}_X(Y, Z)$ commuti il diagramma (1) della Definizione 1.1.4. Per $[s] \in X_{\mathcal{F}_Y}$, sia $x \in X$ tale che $[s] \in \mathcal{F}_{Y,x}$. Sia U un intorno aperto e connesso di x uniformemente rivestito da $p : Y \to X$. Possiamo assumere che s sia una sezione di p su U. Definiamo $\Phi_Y([s]) := s(x) \in p^{-1}(x) \subset Y$. È una buona definizione: se V è un altro intorno aperto di x e t è una sezione di p su V tale che $[t] = [s]$ in $\mathcal{F}_{Y,x}$, allora $s(x) = t(x)$. Per definizione Φ_Y rispetta le fibre ed è continua: se $U \subset Y$ è aperto allora $\Phi_Y^{-1}(U) = \bigcup_{u \in U} \{[s] \in \mathcal{F}_{Y,p(u)} \mid s(p(u)) = u\} = \bigcup_{u \in U} i_{s_u}(p(u)) = i_{s_u}(p(U))$ è aperto, dove s_u è l'unica sezione, su un intorno aperto connesso e uniformemente rivestito di $p(u)$, tale che $s_u(p(u)) = u$. Quindi Φ_Y è un morfismo di rivestimenti. Per il Lemma 3.2.6 è anche una mappa aperta, quindi per vedere che è un isomorfismo di rivestimenti resta solo da vedere che è biiettiva. Per la suriettività, dato $y \in Y$ e un intorno connesso U di y tale che $p(U)$ sia connesso e uniformemente rivestito, allora $s = p_{|U}^{-1}$ è una sezione su $p(U)$ tale che $[s] \in \mathcal{F}_{Y,p(y)}$ e $\Phi_Y([s]) = y$. Per l'iniettività, se $\Phi([s]) = y = \Phi([t])$ allora $[s], [t] \in \mathcal{F}_{Y,p(y)}$ e preso un intorno aperto connesso e uniformemente rivestito V di $p(y)$ deve essere $s_{|V} = t_{|V}$, da cui

$[s] = [t]$. Infine, vale $\Phi_Z \circ R(S(f)) = f \circ \Phi_Y$: per $[s] \in \mathcal{F}_{Y,x} \subset X_{\mathcal{F}_Y}$ si ha $R(S(f))([s]) = [f \circ s]$ e $\Phi_Z([s]) = f(s(x)) = f(\Phi([s]))$, come richiesto.

Definiamo ora un isomorfismo di funtori $\Psi : \mathrm{id}_{\mathcal{D}} \to S \circ R$. Sia F un fascio localmente costante su X. Per dare un morfismo di fasci $\Psi_F : F \to \mathcal{F}_{X_F}$, definiamo una mappa $\Psi_{F,U} : F(U) \to \mathcal{F}_{X_F}(U)$ per ogni $U \subset X$ aperto ponendo $\Psi_{F,U}(s) := i_s$. La mappa $\Psi_{F,U}$ è iniettiva: se $i_s = i_t$ significa che $[s] = [t]$ in F_x per ogni $x \in U$. Per ogni $x \in U$ esiste quindi un intorno aperto U_x di x contenuto in U tale che $s_{|U_x} = t_{|U_x}$. Ma dato che $\bigcup_{x\in U} U_x = U$ deve essere $s = t$. È anche suriettiva: sia $\sigma \in \mathcal{F}_{X_F}$ e sia $\{U_j\}_{j\in J}$ un ricoprimento di U di aperti connessi tali che, su U_j, F sia il fascio costante $\mathcal{F}_{S_j}$, per S_j spazio discreto. Per quanto abbiamo visto prima $p_{\mathcal{F}}^{-1}(U_j) = \bigcup_{s\in F(U_j)} i_s(U_j)$ e $\sigma(U_j)$ deve coincidere con $i_{s_j}(U_j)$ per un qualche $s_j \in F(U_j)$. Ma allora $\sigma_{|U_j} = s_j$. Le sezioni s_j sono compatibili, quindi esiste $s \in F(U)$ tale che $s_{|U_j} = s_j$, da cui $\sigma = i_s = \Psi_{F,U}(s)$. Infine, siano G un altro fascio localmente costante su X e $f : F \to G$ un morfismo di fasci. Chiamiamo $\phi := \bigcup_{x\in X} f_x : X_F \to X_G$ la mappa indotta da f e, per $U \subset X$ aperto, $g_U : \mathcal{F}_{X_F}(U) \to \mathcal{F}_{X_G}(U)$ la mappa $\sigma \mapsto \phi \circ \sigma$. Dobbiamo mostrare che, per ogni $s \in F(U)$, si ha $\Psi_{G,U}(f_U(s)) = g_U(\Psi_{F,U}(s))$. Per $x \in U$ si ha $\Psi_{G,U}(f_U(s))(x) = \Psi_{G,U}(f_U(s)(x)) = [f_U(s)] \in G_x$ e $g_U(\Psi_{F,U}(s))(x) = g_U(i_s(x)) = \phi([s])$ con $[s] \in F_x$, che è proprio $f_x([s]) = [f_U(s)] \in G_x$.

Per il Lemma 1.1.6 i funtori Φ e Ψ^{-1} danno un'equivalenza di categorie. □

Combinando questo risultato con il Teorema 3.3.4 abbiamo il seguente corollario.

Corollario 3.4.2. *La categoria dei fasci localmente costante su X è equivalente alla categoria dei $\pi_1(X, x)$-insiemi sinistri.*

4 Superfici di Riemann

Vogliamo ora presentare un collegamento, non solo "estetico", tra le due teorie sviluppate nei precedenti capitoli. Per farlo abbiamo bisogno di oggetti che siano, in un certo senso, sia algebrici che topologici. Questi oggetti saranno le superfici di Riemann. Consideriamo l'esempio seguente.

Esempio 4.0.3. Siano $\dot{D} := \{z \in \mathbb{C} \,|\, 0 < |z| < 1\}$ e $H := \{z \in \mathbb{C} \,|\, \Re(z) < 0\}$. Sia $p : H \to \dot{D}$ la mappa definita ponendo $p(z) := e^z$. Allora $p : H \to \dot{D}$ è un rivestimento universale: p è suriettiva, perché se $w = \rho e^{i\theta} \in \dot{D}$, con $\rho, \theta \in \mathbb{R}$, allora $p(\log(\rho) + i\theta) = w$ e un intono uniformemente rivestito di w è, per esempio, $U_\theta := \{re^{i\varphi} \,|r, \varphi \in \mathbb{R},\ 0 < r < 1,\ \theta - \pi < \varphi < \theta + \pi\}$. Infine, H è semplicemente connesso.

Consideriamo ora la mappa $p_k : \dot{D} \to \dot{D}$ definita ponendo $p_k(z) := z^k$. Si può verificare che $p_k : \dot{D} \to \dot{D}$ è un rivestimento a k-fogli e che tutti i rivestimenti di $\dot{D}$ sono di questa forma, oppure della forma $p : H \to \dot{D}$ (si vedano il successivo Lemma 4.2.3 e [1], Theorem 5.10).

Per le definizioni e i risultati di analisi complessa rimandiamo a [7], Chapter 10 e successivi.

4.1 Superfici di Riemann, Mappe e Funzioni Olomorfe

Definizione 4.1.1. Sia X uno spazio di Hausdorff. Una *carta complessa* su X è una coppia (U, f) dove $U \subset X$ è aperto e $f : U \to \mathbb{C}$ è un omeomorfismo sulla sua immagine. Due carte complesse (U, f) e (V, g) su X si dicono *compatibili* se le *mappe di transizione* $f \circ g^{-1} : g(U \cap V) \to \mathbb{C}$ e $g \circ f^{-1} : f(U \cap V) \to \mathbb{C}$ sono olomorfe. Una carta complessa (U, f) è detta *centrata* in $y \in U$ se $f(y) = 0$.

Un *atlante complesso* su X è un insieme $\{(U_i, f_i)\}_{i\in I}$ di carte complesse a due a due compatibili tale che $\{U_i\}_{i\in I}$ sia un ricoprimento di X. Due atlanti complessi su X si dicono *equivalenti* o *compatibili* se la loro unione è un atlante complesso su X. La compatibilità è chiaramente una relazione d'equivalenza.

Una classe di equivalenza di atlanti complessi su X è detta *struttura complessa* su X. Una *superficie di Riemann* è uno spazio di Hausdorff dotato di una struttura complessa.

Esempio 4.1.2.

1. Un sottoinsieme $U \subset \mathbb{C}$ aperto è una superficie di Riemann con l'atlante dato dall'unica carta (U, ι), dove $\iota : U \to \mathbb{C}$ è l'inclusione. In particolare, $\mathbb{C}$ è una superficie di Riemann.

2. Sia $\mathbb{P}^1\mathbb{C} = \mathbb{C} \cup \{\infty\}$ la retta proiettiva complessa. Siano $U_\infty = \mathbb{P}^1\mathbb{C} \setminus \{\infty\}$ e $U_0 = \mathbb{P}^1\mathbb{C} \setminus \{0\}$. Siano $f_\infty = \mathrm{id}_{\mathbb{C}} : U_\infty \to \mathbb{C}$ e $f_0 : U_0 \to \mathbb{C}$ definita ponendo $f_0(z) = \frac{1}{z}$ se $z \neq \infty$ e $f_0(\infty) = 0$. Consideriamo l'atlante su $\mathbb{P}^1\mathbb{C}$ dato da $\{(U_i, f_i) \,|\, i \in \{0, \infty\}\}$. Le mappe di transizione, dove definite, sono date da $z \mapsto \frac{1}{z}$ e sono quindi olomorfe. Quindi $\mathbb{P}^1\mathbb{C}$ è una superficie di Riemann *compatta*.

Definizione 4.1.3. Siano Y e X superfici di Riemann. Una mappa continua $\varphi : Y \to X$ è detta *mappa olomorfa* se esistono carte complesse (V, g) su Y e (U, f) su X tali che $\varphi(V) \subset U$ e che la mappa $f \circ \varphi \circ g^{-1} : g(V) \to \mathbb{C}$ (detta *espressione locale* di φ) sia olomorfa.

Una *funzione olomorfa* su X è una mappa olomorfa da X in $\mathbb{C}$.

Una *funzione meromorfa* su X è una mappa olomorfa $\varphi : X \setminus S \to \mathbb{C}$, dove $S \subset X$ è chiuso e discreto, tale che per ogni carta complessa (U, f) la mappa $f \circ \varphi^{-1} : \varphi(U \setminus S) \to \mathbb{C}$ sia meromorfa su $\varphi(U)$.

Le superfici di Riemann con le mappe olomorfe formano una categoria. Un isomorfismo tra superfici di Riemann (cioè un mappa olomorfa e biiettiva con inversa olomorfa) è anche detta *mappa biolomorfa*.

Osservazione 4.1.4. Siano X una superficie di Riemann e $\varphi : X \to \mathbb{C}$ una funzione meromorfa. Ponendo $\varphi(p) = \infty$ per ogni polo p di φ si ottiene una mappa olomorfa $\varphi : X \to \mathbb{P}^1\mathbb{C}$. Viceversa, una mappa olomorfa $\varphi : X \to \mathbb{P}^1\mathbb{C}$, non ovunque ∞, è una funzione meromorfa su X (si veda [1], Theorem 1.15).

Nel resto di questa sezione e nella prossima assumeremo che tutte le mappe tra superfici di Riemann siano *non costanti sulle singole componenti connesse*, cioè che l'immagine di una componente connessa non sia un solo punto. Vediamo che tutte le mappe tra superfici di Riemann sono, localmente, della forma dell'Esempio 4.0.3.

Proposizione 4.1.5. *Siano Y e X superfici di Riemann e $\varphi : Y \to X$ una mappa olomorfa, non costante sulle singole componenti connesse di Y. Siano $y \in Y$ e $x = \varphi(y)$. Allora esistono carte locali (V_y, g_y) centrata in y e (U_x, f_x) centrata in x tali che $\varphi(V_y) \subset U_x$ e $f_x \circ \varphi \circ g_y^{-1} = p_k$, dove $p_k(z) = z^k$. Inoltre, l'intero k non dipende dalle carte V_x e U_y scelte.*

Dimostrazione. Tramite trasformazioni lineari e restringendo V_y e U_x se necessario, si possono trovare carte locali (V'_y, g'_y) e (U_x, f_x) centrate in y e in x rispettivamente e tali che $\varphi(V_y) \subset U_x$. Considerando lo sviluppo in serie di Taylor di $T := f_x \circ \varphi \circ g'^{-1}_y$ si ha che T è della forma $T(z) = z^k H(z)$ per qualche H olomorfa tale che $H(0) \neq 0$ e k intero positivo, dato che $T(0) = 0$. Dalla discretezza degli zeri di H, esiste un intorno $V''_y \subset V'_y$ di y tale che H non si annulli in alcun punto di $g'_y(V''_y)$. Allora esiste $h : g'_y(V''_y) \to \mathbb{C}$ olomorfa e tale che $H = \exp \circ h$ (si noti che possiamo assumere V''_y semplicemente connesso e quindi applicare [7], Theorem 13.18), quindi $R : g'_y(V''_y) \to \mathbb{C}$ definita ponendo $R(z) := \exp(h(z)/k)$ è tale che $R^k = H$ su $g'_y(V''_y)$. Abbiamo allora $T(z) = (\eta(z))^k$, dove $\eta(z) := zR(z)$. Da $\eta'(0) = R(0) \neq 0$ si ha che esiste un intorno $V_y \subset V''_y$ di y tale che η sia invertibile su $g'_y(V_y)$, con inversa olomorfa ([7], Theorem 10.34). Allora, posto $g_y := \eta \circ g'_y$, si ha che (V_y, g_y) è una carta centrata in y tale che $\varphi(V_y) \subset U_x$. Inoltre $(f_x \circ \varphi \circ g_y^{-1})(z) = T(\eta^{-1}(z)) = z^k$, come richiesto.

Per l'unicità di k, osserviamo che per $p \in f_x^{-1}(B) \setminus \{x\}$, dove $B \subset f_x(U_x)$ è una palla aperta centrata in 0, si ha $k = |p_k^{-1}(f_x(p))| = |\varphi^{-1}(p)|$, dato che g_y è biiettiva. Ma la cardinalità di questo insieme è indipendente dalle carte complesse considerate. □

Definizione 4.1.6. L'intero k della proposizione precedente è detto *ordine di ramificazione* di φ in y. I punti di y con ordine di ramificazione maggiore di 1 sono detti *punti di ramificazione* di φ. L'insieme dei punti di ramificazione di φ sarà denotato da S_φ.

Corollario 4.1.7. *Sia $\varphi : Y \to X$ olomorfa e non costante su ciascuna componente connessa di Y. Allora φ è aperta e le fibre di φ e S_φ sono sottoinsiemi chiusi e discreti di Y.*

Dimostrazione. La prima parte deriva dal fatto che $z \mapsto z^k$ è aperta ([7], Theorem 10.32). La fibra di $x \in X$ è discreta, altrimenti $\varphi^{-1}(x)$ avrebbe un punto di accumulazione; ma allora per il principio di identità ([7], Theorem 10.18) qualche espressione locale di φ sarebbe costante, quindi lo sarebbe anche φ. Infine S_φ è discreto e non ha punti di accumulazione, perché ogni punto y ha un intorno (V_y nella Proposizione 4.1.5) in cui non ci sono punti di ramificazione (escluso eventualmente y). □

Corollario 4.1.8. *Una mappa olomorfa biiettiva $\varphi : Y \to X$ è biolomorfa.*

Dimostrazione. Data l'iniettività di φ, non ci sono punti di ramificazione, quindi φ^{-1} è continua ed olomorfa, perché la sua espressione locale rispetto a carte come nella Proposizione 4.1.5 è l'identità. □

4.2 Rivestimenti Ramificati

Ricordiamo che una mappa continua tra spazi topologici si dice *propria* se la controimmagine di ogni compatto è compatta. Se gli spazi in questione sono di Hausdorff e il dominio è compatto, ogni mappa continua è anche propria: i compatti in uno spazio Hausdorff sono chiusi e la loro controimmagine è chiusa in un compatto, quindi compatta. Inoltre, un rivestimento finito $p : Y \to X$ è una mappa propria: se $Z \subset X$ è compatto e $\mathcal{U}$ è un ricoprimento di aperti di $p^{-1}(Z)$, possiamo raffinarlo in modo che $p_{|U}$ sia biiettiva per ogni $U \in \mathcal{U}$. Dato che p è aperta, $\{p(U) \mid U \in \mathcal{U}\}$ è un ricoprimento di aperti di Z, da cui possiamo estrarre un sottoricoprimento finito, da cui otteniamo un sottoricoprimento finito di $\mathcal{U}$.

Definizione 4.2.1. Siano Y e X spazi di Hausdorff localmente compatti. Una mappa continua $p : Y \to X$ che sia propria e suriettiva è detta *rivestimento ramificato* se esiste $Y' \subset Y$ tale che $Y \setminus Y'$ sia discreto e che $p_{|Y'} : Y' \to p(Y')$ sia un rivestimento. Un rivestimento ramificato è detto *finito* (rispettivamente *di grado* k, o *di Galois*) se $p_{|Y'} : Y' \to p(Y')$ è finito (rispettivamente a k fogli, o di Galois).

Proposizione 4.2.2. *Siano Y e X superfici di Riemann con X connesso e sia $f : Y \to X$ una mappa olomorfa propria e non costante su ciascuna componente connessa di Y. Allora $f : Y \to X$ è un rivestimento ramificato finito.*

Dimostrazione. Notiamo innanzitutto che Y e X sono di Hausdorff e localmente compatti, perché localmente omeomorfi a $\mathbb{C}$. Per il Corollario 4.1.7 $f(Y)$ è aperto in X, quindi per avere la suriettività, dato che X è connesso, resta da vedere che $f(Y)$ è anche chiuso. Sia $x \in X \setminus f(Y)$. Dato che X è localmente compatto, esiste un intorno aperto U di x con $\overline{U}$ compatto. Allora $f(f^{-1}(\overline{U}))$ è compatto, quindi chiuso (perché X è di Hausdorff). Allora $U \setminus f(f^{-1}(\overline{U}))$ è un intorno aperto di x disgiunto da $f(Y)$.

Sia $Y' := Y \setminus S_f$ e sia $x \in X \setminus f(S_f)$. Per la Proposizione 4.1.5 ogni punto $y \in f^{-1}(x)$ ha un intorno V_y omeomorfo ad $f(V_y)$. Dato che per il Corollario 4.1.7 le fibre sono finite, $U := \bigcap_{y \in f^{-1}(x)} f(V_y)$ è un intorno aperto di x uniformemente rivestito. Quindi $f_{|Y'} : Y' \to f(Y')$ è un rivestimento finito. $\square$

Lemma 4.2.3. *Sia $p : Y \to X$ un rivestimento connesso. Se X è una superficie di Riemann, esiste un'unica struttura complessa su Y tale che p sia una mappa olomorfa.*

Dimostrazione. Sia $y \in Y$ e sia V un intorno aperto di y tale che $p_{|V} : V \to p(V)$ sia un un omeomorfismo. Sia (U, f) una carta complessa su X con $U \subset p(V)$. Allora $\mathcal{C}_y := (V, f \circ p)$ è una carta complessa su Y con $y \in V$. Procedendo in questo modo otteniamo un atlante $\mathcal{U} := \{\mathcal{C}_y \mid y \in Y\}$: le carte sono compatibili perché lo sono quelle su X. Per l'unicità, sia $\mathcal{V}$ un altro atlante su Y tale che p sia olomorfa e siano $(U, f) \in \mathcal{U}$ e $(V, g) \in \mathcal{V}$ carte complesse e $y \in U \cap V$. Siano inoltre (W, h) una carta complessa su X con W intorno di $p(y)$ uniformemente rivestito e $N := U \cap V \cap W_y$, dove W_y è la componente connessa di $p^{-1}(W)$ con $y \in W_y$. Allora $p_{|N}$ è biolomorfa da N sulla sua immagine per il Corollario 4.1.8 e quindi lo sono anche $h \circ p_{|N} \circ g^{-1}$ e $h \circ p_{|N} \circ f^{-1}$. Ma allora $(h \circ p_{|N} \circ f^{-1})^{-1} \circ h \circ p_{|N} \circ g^{-1} = f \circ g^{-1}$ è olomorfa su N. Data l'arbitrarietà di $y \in U \cap V$ lo è su tutto $U \cap V$, quindi le due carte sono compatibili. $\square$

Siano X una superficie di Riemann connessa, $S \subset X$ un sottoinsieme chiuso e discreto e $X' = X \setminus S$. Denotiamo con $\mathrm{Hol}_{X,S}$ la categoria i cui oggetti sono superfici di Riemann Y equipaggiate con una mappa olomorfa propria $p : Y \to X$, non costante su ciascuna componente connessa di Y, tale che $S_p \subset p^{-1}(S)$ e i cui morfismo sono mappe olomorfe compatibili con le proiezioni. Più precisamente, se $p : Y \to X$ e $q : Z \to X$ sono due oggetti in questa categoria, un morfismo tra di loro è dato da una mappa olomorfa $f : Y \to Z$ tale che $q \circ f = p$.

Teorema 4.2.4. *C'è un'equivalenza di categorie tra $\mathrm{Hol}_{X,S}$ e i rivestimenti finiti di $X' := X \setminus S$.*

Dimostrazione. Sia $\mathcal{F}$ il funtore che manda un oggetto $p : Y \to X$ di $\mathrm{Hol}_{X,S}$ in $p' := p_{|Y'} : Y' \to X'$, dove $Y' := Y \setminus p^{-1}(S)$, e un morfismo $f : Y \to Z$ in $f' := f_{|Y'}$. Quest'ultimo è un morfismo di rivestimenti tra Y' e Z' (dove $Z' := Z \setminus q^{-1}(S)$), perché per definizione $f'(Y') \subset Z'$ ed è compatibile con le proiezioni $p' := p_{|Y'} : Y' \to X'$ e $q' := q_{|Z'} : Z' \to X'$.

Per l'essenziale suriettività, sia $p' : Y' \to X'$ un rivestimento e mostriamo che esistono una superficie di Riemann $Y \supset Y'$ e una mappa olomorfa propria $p : Y \to X$ tali che $p_{|Y'} = p'$ e $Y \setminus p^{-1}(S) = Y'$. Possiamo assumere che Y' sia connesso: se così non fosse, basta decomporlo in componenti connesse $\coprod_i Y'_i$, trovare superfici di Riemann opportune Y_i e porre $Y := \coprod_i Y_i$. Siano $x \in S$ e (U_x, f_x) una carta complessa centrata in x tale che $U_x \cap S = \{x\}$ e $f_x(U_x) = D = \{z \in \mathbb{C} \mid |z| < 1\}$. Decomponiamo

$p'^{-1}(U_x \setminus \{x\})$ in componenti connesse $\coprod_{i\in I_x} V_x^i$. Ogni $f_x \circ p'_{|V_x^i} : V_x^i \to \dot{D} = D \setminus \{0\}$ è un rivestimento finito, quindi per l'Esempio 4.0.3 (si veda [1], Theorem 5.10) esiste una mappa biolomorfa $\rho_x^i : V_x^i \to \dot{D}$ tale che $f \circ (f_x \circ p'_{|V_x^i})^{-1} = p_k$, dove $p_k(z) = z^k$. Scegliamo ora, per ogni $x \in S$ e $i \in I_x$, punti $y_x^i \notin Y'$. Definiamo $Y := Y' \cup \coprod_{i,x}\{y_x^i\}$, un'estensione $p : Y \to X$ di p' ponendo $p(y_x^i) := x$ e estensioni (biiettive) $\overline{\rho}_x^i : V_x^i \cup \{y_x^i\} \to D$ di ρ_x^i ponendo $\overline{\rho}_x^i(y_x^i) := 0$. Diamo a Y l'unica topologia tale che tutte le $\overline{\rho}_x^i$ siano continue e aperte (quindi omeomorfismi). Definiamo inoltre una struttura complessa su Y aggiungendo alle carte su Y' date dalla struttura complessa del Lemma 4.2.3 le carte $(V_x^i, \overline{\rho}_x^i)$. Queste carte sono compatibili, perché se (U, f) è una carta su Y' (da cui $y_x^i \notin U$) allora $\overline{\rho}_x^i \circ f^{-1} = \rho_x^i \circ f^{-1}$ e la sua inversa sono olomorfe, perché ρ_x^i è biolomorfa. La mappa $p : Y \to X$ è olomorfa, perché su Y' coincide con p' nell'intorno V_x^i di y_x^i la sua espressione locale è p_k. Infine, p è propria, perché p' lo è e le sue fibre sono finite, quindi controimmagini di compatti di X sono controimmagini di compatti di X' unite ad un insieme finito di punti di Y.

$\mathcal{F}$ è pienamente fedele: siano Y e Z come all'inizio della dimostrazione e $\varphi' : Y' \to Z'$ un morfismo di rivestimenti. Per il Lemma 3.2.6 $\varphi' : Y' \to Z'$ è un rivestimento, quindi per il Lemma 4.2.3 c'è un'unica struttura complessa su Y' tale che φ' sia olomorfa. Questa è compatibile con quella di Y: $p' = q \circ \varphi'$ è olomorfa rispetto ad entrambe, quindi per il Lemma 4.2.3 applicato a $p' : Y' \to X'$ devono coincidere. Sia $y \in Y \setminus Y'$. Abbiamo visto y ha un intorno V biolomorfo a D; possiamo assumere che $p'(V \setminus \{y\})$ sia uniformemente rivestito sia da p' che da q'. Allora $W := \varphi'(V \setminus \{y\}) \subset q'^{-1}(p'(V \setminus \{y\}))$ è biolomorfo a $\dot{D}$ ed esiste quindi un unico $z \in Z \setminus Z'$ tale che $W \cup \{y\}$ sia biolomorfo a D. Ponendo $\varphi(y) := z$ e ripetendo per ogni $y \in Y \setminus Y'$ otteniamo una mappa $\varphi : Y \to Z$. Similmente a prima si verifica che φ è l'unica mappa olomorfa tale che $\mathcal{F}(\varphi) = \varphi_{|Y'} = \varphi'$. □

Osservazione 4.2.5. Con le notazioni della dimostrazione precedente, abbiamo che la mappa $\sigma \mapsto \sigma_{|Y'}$ induce un isomorfismo tra $\mathrm{Aut}(Y|X)$ (in $\mathrm{Hol}_{X,S}$) e $\mathrm{Aut}(Y'|X')$ (come rivestimento). In particolare, Se $p' : Y' \to X'$ è di Galois, allora l'azione di $\mathrm{Aut}(Y|X)$ sulle fibre di p è transitiva (per continuità degli automorfismi). Di conseguenza se $y \in Y$ tutti gli elementi di $p^{-1}(p(y))$ hanno lo stesso ordine di ramificazione.

4.3 Estensioni di Campi e Rivestimenti

Denotiamo con $\mathcal{M}(X)$ l'insieme delle funzioni meromorfe su una superficie di Riemann X. Notiamo che $\mathcal{M}(X)$ è un anello commutativo, con le operazioni di somma e prodotto indotte da $\mathbb{C}$. Lo zero di questo anello è la funzione costante 0 mentre la funzione costante 1 è l'unità.

Lemma 4.3.1. *Se X è una superficie di Riemann connessa, $\mathcal{M}(X)$ è un campo.*

Dimostrazione. Sia $f \in \mathcal{M}(X)$ non nulla. Notiamo che se gli zeri di f sono un sottoinsieme chiuso e discreto di X allora $1/f \in \mathcal{M}(X)$: infatti è olomorfa su $X \setminus f^{-1}(0)$. Supponiamo per assurdo che gli zeri di f non siano discreti. Dato che per l'Osservazione 4.1.4 f è una mappa olomorfa da X a $\mathbb{P}^1\mathbb{C}$, questo contraddice il Corollario 4.1.7, dove avevamo supposto che le mappe fossero non costanti su ogni componente connessa. Ma allora f deve essere costante su X, che è connessa, quindi $f = 0$, assurdo. □

Una mappa olomorfa tra superfici di Riemann $\varphi : Y \to X$, non costante su ogni componente connessa di Y, induce un morfismo di anelli $\varphi^* : \mathcal{M}(X) \to \mathcal{M}(Y)$ dato da $f \mapsto f \circ \varphi$. Vogliamo mostrare che, Se X e Y sono compatti e X è connesso, allora $(\mathcal{M}(Y), \varphi^*)$ è un'algebra étale su $\mathcal{M}(X)$. Notiamo che φ^* è iniettiva, perché φ è suriettiva, quindi se $f \neq 0$ vale anche $\varphi^*(f) \neq 0$. Dove non specificato assumeremo quindi $\mathcal{M}(X) \subset \mathcal{M}(Y)$. Per compattezza, Y si decompone in un unione disgiunta finita di superfici di Riemann connesse $Y = \coprod_i Y_i$, quindi $\mathcal{M}(Y) = \prod_i \mathcal{M}(Y_i)$. È quindi sufficiente dimostrare che, nel caso Y sia connessa, $\mathcal{M}(Y)|\mathcal{M}(X)$ è un'estensione di campi finita. Tale estensione sarà sicuramente separabile, perché le funzioni costanti formano un sottocampo di $\mathcal{M}(X)$ isomorfo a $\mathbb{C}$, quindi $\mathcal{M}(X)$ è perfetto.

Proposizione 4.3.2. *Siano Y e X superfici di Riemann compatte e connesse e sia $\varphi : Y \to X$ una mappa olomorfa propria non costante. L'estensione di campi $\mathcal{M}(Y)|\mathcal{M}(X)$ è finita. Inoltre, se Y soddisfa*

(*) *per ogni $y_1, \dots, y_n \in Y$ e $a_1, \dots, a_n \in \mathbb{C}$ esiste $f \in \mathcal{M}(Y)$ tale che $f(y_i) = a_i$ per ogni $i = 1, \dots, n$*

il grado dell'estensione è lo stesso di φ come rivestimento ramificato.

Dimostrazione. Mostriamo che ogni $f \in \mathcal{M}(Y)$ è radice di un polinomio (non necessariamente irriducibile) di grado d a coefficienti in $\mathcal{M}(X)$. Siano d il grado di φ come rivestimento ramificato, S l'insieme dei punti di ramificazione di Y, $Y' := Y \setminus S$ e $X' := X \setminus \varphi(S)$. Per ogni $x \in X'$ sia $U_x \subset X'$ un intorno di x uniformemente rivestito da una famiglia $\{V_{x,1}, \ldots, V_{x,d}\}$ di aperti di Y. Per il Corollario 4.1.8 le mappe $s_{x,i} := (\varphi_{|V_{x,i}})^{-1}$ sono olomorfe su U_x, così come le $f_{x,i} := f \circ s_{x,i}$. Definiamo il polinomio F_x a coefficienti in $\mathcal{M}(U_x)$ ponendo $F_x(t) := \prod_{i=1}^{d}(t - f_{x,i})$. Ora se $x_1 \neq x_2$ sono due punti distinti di X' con $U_{x_1} \cap U_{x_2} \neq \emptyset$ deve essere $F_{x_1} = F_{x_2}$ in $\mathcal{M}(U_{x_1} \cap U_{x_2})[t]$, perché le loro radici sono funzioni meromorfe che coincidono su $U_{x_1} \cap U_{x_2}$. Allora i coefficienti di F_x si estendono a funzioni b_i meromorfe su tutto X' e il polinomio $F(t) := t^d + b_{d-1}t^{d-1} + \cdots + b_0$ ha coefficienti in $\mathcal{M}(X')$. Per estendere le b_i a tutto X, siano $x \in \varphi(S)$, $y \in \varphi^{-1}(x)$ e (U_x, f_x), (U_y, f_y) carte centrate in x e y rispettivamente. Dato che $(f_x \circ \varphi)(y) = 0$, esiste un intero k tale che, posto $g := (f_x \circ \varphi \circ f_y^{-1})^k (f \circ f_y^{-1}) : f_y(U_y) \to \mathbb{C}$, si abbia $\lim_{z \to 0} zg(z) = 0$. Inoltre g è olomorfa in un intorno di 0, quindi 0 è una singolarità eliminabile per $g = ((f_x \circ \varphi)^k f) \circ f_y^{-1}$ ([7], Theorem 10.20). Possiamo allora assumere g olomorfa in 0. Quindi $(f_x \circ \varphi)^k f$ è olomorfa in y, da cui abbiamo che le b_i sono olomorfe in x. Concludiamo che $F \in \mathcal{M}(X)[t]$ e dato che in ogni $x \in X$ in U_x si ha $(F \circ s_{x,i})(f \circ s_{x,i}) = F(f_{x,i}) = 0$, vale $F(f) = 0$.

Dato che tutti gli elementi di $\mathcal{M}(Y)$ hanno grado al più d su $\mathcal{M}(X)$, l'estensione deve essere finita: se supponiamo $f \in \mathcal{M}(Y)$ di grado massimo, per il Teorema 2.1.3 per ogni $g \in \mathcal{M}(Y)$ deve valere $\mathcal{M}(X)(f, g) = \mathcal{M}(X)(h)$ per qualche $h \in \mathcal{M}(Y)$. Ma dato che h ha al più lo stesso grado di f deve valere $g \in \mathcal{M}(X)(f)$, da cui $\mathcal{M}(Y) = \mathcal{M}(X)(f)$.

Supponiamo ora che Y soddisfi (*) e mostriamo che esiste $f \in \mathcal{M}(Y)$ radice di un polinomio irriducibile di grado d a coefficienti in $\mathcal{M}(X)$. Siano $x \in X'$ e $\{y_1, \ldots, y_d\} = \varphi^{-1}(x)$ e sia $f \in \mathcal{M}(Y)$ tale che $f(y_i) \neq f(y_j)$ per $i \neq j$. Sia $F(t) = a_n t^n + \cdots + a_0 \in \mathcal{M}(X)[t]$ irriducibile tale che $F(f) = 0$, con $n \leq d$. Se i coefficienti a_i fossero funzioni olomorfe in x il polinomio $a_n(x)t^n + \cdots + a_0(x) \in \mathbb{C}[t]$ avrebbe d radici distinte $f(y_1), \ldots, f(y_d)$ e quindi sarebbe $n = d$. Se qualche a_i ha un polo in x, basta sostituire x con un $\tilde{x} \in U_x$ tale che f abbia ancora valori distinti nelle controimmagini di $\tilde{x}$. □

La condizione (*) è in realtà sempre verificata, come conseguenza del *Riemann Existence Theorem*. La dimostrazione di questo fatto non è però elementare. Si veda [1], Corollary 14.13. Nel seguito (Teorema 4.3.4 e corollari) assumeremo questo risultato.

In seguito, dato $F(t) = a_n t^n + \cdots + a_0 \in \mathcal{M}(X)[t]$ e $x \in X$ che non sia un polo per nessuno dei coefficienti di F, indicheremo con F_x in polinomio in $a_n(x)t^n + \cdots a_0(x) \in \mathbb{C}[t]$.

Lemma 4.3.3. *Siano X una superficie di Riemann e $F \in \mathcal{M}(X)[t]$ ed $x \in X$ come sopra. Se F_x ha zeri distinti $z_1, \ldots, z_n$ esistono un intorno V di x e $f_1, \ldots, f_n \in \mathcal{M}(V)$ tali che $F = \prod_i (t - f_i)$ in $\mathcal{M}(V)[t]$ e $f_1(x'), \ldots, f_n(x')$ sono gli zeri di $F_{x'}$ per $x' \in V$.*

Dimostrazione. Osserviamo innanzitutto che per $V \subset X$ aperto $\mathcal{M}(V)$ è una $\mathcal{M}(X)$-algebra tramite la restrizione, quindi ha senso considerare F come un polinomio a coefficienti in $\mathcal{M}(V)$.

Sia (U, ψ) una carta centrata in x. Per la discretezza dei poli dei coefficienti a_i possiamo trovare una palla aperta $D \subset \psi(U)$ centrata in 0 tale che i $b_i := a_i \circ \psi^{-1}$ siano olomorfi in tutti i punti di $\overline{D}$. Per la discretezza degli zeri di F_x, per ogni $j = 1, \ldots, n$ possiamo trovare una palla aperta B_j centrata in z_j tale che F_x non abbia altri zeri in $\overline{B_j}$. Indichiamo con $G : D \times \mathbb{C} \to \mathbb{C}$ la mappa continua $G(z, t) := F_{\psi^{-1}(z)}(t) = b_n(z)t^n + \cdots + b_0(z)$. Dato che G non si annulla in $\{0\} \times \partial B_j$, esiste una palla aperta $D_j \subset D$ centrata in 0 tale che G non si annulli in $D_j \times \partial B$. Per il Principio dell'Argomento ([7], Theorem 10.30) e il Teorema dei Residui ([7], Theorem 10.29) il numero di zeri, contati con molteplicità, di $F_{x'}$ al variare di $x' \in \psi^{-1}(D_j)$, è dato da

$$n(z) := \frac{1}{2\pi i} \int_\gamma \frac{F'_{x'}(w)}{F_{x'}(w)} \mathrm{d}w = \frac{1}{2\pi i} \int_\gamma \frac{\partial G(z, w)}{\partial w} \frac{1}{G(z, w)} \mathrm{d}w$$

dove $\gamma : [0, 1] \to \mathbb{C}$ è una parametrizzazione positiva (in senso antiorario) di ∂B_j e $z := \psi(x')$. Dato che n è continua su D_j a valori in $\mathbb{Z}$ e $n(0) = 1$ deve essere $n(z) = 1$ per ogni $z \in D_j$. Sia $\varphi_j(z)$ l'unico zero di $F_{x'}$ in B_j. Dato che $g_z(w) := (w - \varphi_j(z)) \frac{F'_{x'}(w)}{F_{x'}(w)}$ è olomorfa in $\overline{B}_j \setminus \{\varphi_j(z)\}$ e ha una singolarità eliminabile in $\varphi_j(z)$ si ha che l'integrale di g_z lungo γ è nullo, quindi

$$\varphi_j(z) = \varphi_j(z)n(z) + \frac{1}{2\pi i} \int_\gamma g_z(w) \mathrm{d}w = \frac{1}{2\pi i} \int_\gamma w \frac{F'_{x'}(w)}{F_{x'}(w)} \mathrm{d}w = \frac{1}{2\pi i} \int_\gamma w \frac{\partial G(z, w)}{\partial w} \frac{1}{G(z, w)} \mathrm{d}w$$

che è olomorfa in D_j. Ponendo $V = \bigcap_{j=1}^n \varphi^{-1}(D_j)$ e $f_j := \varphi_j \circ \psi$ si ha la tesi. □

Teorema 4.3.4. *Sia X una superficie di Riemann compatta e connessa. C'è un'anti-equivalenza tra la categoria delle superfici di Riemann compatte Y equipaggiate con una mappa olomorfa $\varphi : Y \to X$, e quella delle algebre étale su $\mathcal{M}(X)$. In questa anti-equivalenza i rivestimenti ramificati connessi corrispondo ad estensioni di campi dello stesso grado e i rivestimenti ramificati di Galois ad estensioni di Galois.*

Dimostrazione. Grazie alla Proposizione 4.3.2, possiamo definire un funtore controvariante $\mathcal{F}$ che manda una superficie di Riemann Y, con mappa olomorfa $\varphi : Y \to X$, nella $\mathcal{M}(X)$-algebra étale $\mathcal{M}(Y)$ e una mappa olomorfa $f : Y \to Z$ in $\mathcal{F}(f) := f^* : \mathcal{M}(Z) \to \mathcal{M}(Y)$. Questo funtore è pienamente fedele: per un cenno di dimostrazione si veda [9], Theorem 3.3.7.

Per l'essenziale suriettività di $\mathcal{F}$, sia L una $\mathcal{M}(X)$-algebra. È sufficiente mostrare la tesi nel caso L sia un campo: altrimenti possiamo decomporre $L = \prod_i L_i$ come prodotto finito di campi, trovare superfici di Riemann Y_i tali che $\mathcal{M}(Y_i) \cong L_i$ per ogni i e concludere ponendo $Y = \coprod_i Y_i$. Assumiamo allora che $L|\mathcal{M}(X)$ sia un'estensione di campi di grado d e siano $\alpha \in L$ un elemento primitivo e F il suo polinomio minimo. Indicando con F' la derivata formale di F, da $\gcd(F, F') = 1$ abbiamo che esistono $A, B \in \mathcal{M}(X)[t]$ tali che $AF + BF' = 1$. Abbiamo allora che può verificarsi $\gcd(F_x, F'_x) \neq 1$ soltanto se x è un polo per uno dei coefficienti di A o di B. Detto S l'insieme dei punti di X che sono poli per qualche coefficiente di A, B o di F abbiamo che F_x ha d radici distinte per ogni $x \in X' := X \setminus S$.

Definiamo un fascio su X' definendo, per $U \subset X'$ aperto, $\mathcal{G}(U)$ come l'insieme delle funzioni olomorfe su U che sono radici di F. Per $x \in X'$, siano V e $f_1, \ldots, f_d$ come nel Lemma precedente. Allora $\mathcal{G}$ ristretto a V è il fascio costante dato da $\{f_1, \ldots, f_d\}$, quindi per il Teorema 3.4.1 abbiamo un rivestimento finito $p_{\mathcal{G}} : X'_{\mathcal{G}} \to X'$. Per il Teorema 4.2.4 esistono quindi una superficie di Riemann $X_{\mathcal{G}}$ e una mappa olomorfa propria $\varphi : X_{\mathcal{G}} \to X$ (quindi $X_{\mathcal{G}} = \varphi^{-1}(X)$ è compatta) tale che $\varphi_{|X'_{\mathcal{G}}} = p_{\mathcal{G}}$. Per vedere che $X_{\mathcal{G}}$ è connessa, sia Z una sua componente connessa e sia $Z' := Z \cap X'_{\mathcal{G}}$. Definiamo una funzione meromorfa f su $\varphi^{-1}(V)$ ponendo $f([f_i]) = f_i(p_{\mathcal{G}}([f_i])) = f_i(x')$ se $x' \in V$ e $[f_i] \in \mathcal{G}_{x'}$. Come nella dimostrazione della Proposizione 4.3.2, possiamo estendere f a tutto Z, quindi $f \in \mathcal{M}(Z)$ ha polinomio minimo di grado al più e, il grado di $\varphi_{|Z} : Z \to X$ come rivestimento ramificato. Ma F è irriducibile e $F(f) = 0$: se $[f_i] \in \mathcal{G}_{x'} \subset Z'$ allora $(F(f))([f_i]) = F_{\varphi([f_i])}(f([f_i])) = F_{x'}(f_i(x')) = 0$ per il Lemma. Allora F deve essere il polinomio minimo di f su $\mathcal{M}(X)$, quindi $e = d$ e si ha che Z è l'unica componente connessa di $X_{\mathcal{G}}$. Infine, dato che $\mathcal{M}(X_{\mathcal{G}})$ ha grado d su $\mathcal{M}(X)$, deve essere $\mathcal{M}(X_{\mathcal{G}}) = \mathcal{M}(X)(f)$ e la mappa $\mathcal{M}(X_{\mathcal{G}}) \to L$ determinata da $f \mapsto \alpha$ è un isomorfismo di campi.

Se Y è connessa $\mathcal{M}(Y)$ è un campo e il grado $\mathcal{M}(Y)|\mathcal{M}(X)$ è lo stesso $\varphi : Y \to X$ come rivestimento ramificato per la Proposizione 4.3.2. Infine, consideriamo il gruppo $\mathrm{Aut}(Y|X)$. Per il Teorema 4.2.4, questo è isomorfo al gruppo di automorfismi H del rivestimento $p : Y' \to X'$ corrispondente. Il gruppo H ha ordine uguale al grado d del rivestimento se e solo se quest'ultimo è di Galois. Questo si verifica se e solo se l'azione di H sulle fibre $p^{-1}(x)$ è transitiva e solo in questo caso H è in biiezione con $p^{-1}(x)$, perché se $gy = hy$ per qualche $g, h \in H$ e $y \in p^{-1}(x)$ deve essere $h = g$ per il Lemma 3.2.1. Dato che $\mathcal{M}(Y)|\mathcal{M}(X)$ è di Galois se e solo se $\mathrm{Gal}(\mathcal{M}(Y)|\mathcal{M}(X))$ ha grado d, concludiamo che $\varphi : Y \to X$ è un rivestimento ramificato di Galois se e solo se l'estensione $\mathcal{M}(Y)|\mathcal{M}(X)$ è di Galois. □

Applicando il Teorema 4.3.4 al caso $X = \mathbb{P}^1\mathbb{C}$ e ricordando l'Osservazione 4.1.4, abbiamo i seguenti corollari ([9], Proposition 3.3.11 e Corollary 3.3.12).

Corollario 4.3.5. *Sia Y una superficie di Riemann compatta e connessa. Allora $\mathcal{M}(Y)$ è un'estensione finita di $\mathbb{C}(t)$, il campo delle funzioni razionali a coefficienti in $\mathbb{C}$ nell'indeterminata t.*

Idea di dimostrazione. Per il teorema d'esistenza esiste una funzione meromorfa non costante su Y, che possiamo vedere come una mappa olomorfa $Y \to \mathbb{P}^1\mathbb{C}$. Resta poi da osservare che $\mathcal{M}(\mathbb{P}^1\mathbb{C}) \cong \mathbb{C}(t)$. □

Corollario 4.3.6. *C'è un'anti-equivalenza tra la categoria delle superfici di Riemann compatte e connesse con mappe olomorfe non costanti e la categoria delle estensioni finite di $\mathbb{C}(t)$ con morfismi di $\mathbb{C}$-algebre.*

È possibile ottenere questi ultimi risultati con metodi più algebrici, validi per varietà su qualunque campo base, come fatto in [8]. Questi argomenti non sono stati approfonditi in questa relazione.

Riferimenti bibliografici

[1] O. Forster, *Lectures on Riemann Surfaces*, Springer-Verlag (1937)

[2] M. J. Greenberg, *Lectures on Algebraic Topology*, W. A. Benjamin (1967)

[3] G. Karpilovski, *Topics in Field Theory*, Nort-Holland Mathematics Studies (1940).

[4] C. Kosniowski, *A First Course in Algebraic Topology*, Cambridge University Press (1980).

[5] S. Mac Lane, *Categories for the Working Mathematician*, Springer-Verlag (1971)

[6] J. S. Rose, *A Course on Group Theory*, Cambridge University Press (1978)

[7] W. Rudin, *Real and Comples Analysis*, McGraw-Hill (1966)

[8] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag (2009)

[9] T. Szamuely, *Galois Groups and Fundamental Groups*, Cambridge University Press (2009).