Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Specialistica in Matematica

GRUPPI PROFINITI ED ESTENSIONI DI GALOIS DI GRADO INFINITO

Tesi di Laurea Specialistica in Matematica

Relatrice:
Chiar.ma Dott.ssa
MARTA MORIGI

Presentata da:
GIACOMO PATRIZI

II Sessione
Anno Accademico 2009-10

Mai appena poco tempo fa avrei immaginato di giungere qui senza te.
Ricordo di quando con orgoglio e presunzione mi mostravi le tue grandi mani scure e callose.
Anche io avrei voluto mostrarti un giorno le mie.
A mio padre.

Indice

Introduzione

Il mio interesse nello studio dei gruppi profiniti è nato durante la preparazione della mia tesi di laurea triennale quando si è esteso il simbolo di Legendre dagli interi agli interi p-adici. Un modo diverso da quello usato nella mia precedente tesi per definire l'insieme degli interi p-adici è quello di vedere i suoi elementi come particolari somme formali infinite e far derivare la sua struttura di gruppo topologico, tramite una biezione, dalla struttura di gruppo topologico di un limite inverso di un particolare sistema inverso di gruppi finiti.

Nei primi due capitoli di questa tesi sono stati trattati alcuni risultati riguardanti gli spazi topologici ed i gruppi topologici, neccessari per poter in seguito derivare alcune proprietà dei sistemi inversi. Nel terzo capitolo vengono definiti i sistemi inversi ed i limiti inversi di sitemi inversi e ne vengono analizzate alcune loro importanti proprietà topologiche. Nel quarto capitolo vengono definiti i gruppi pro-$\mathcal{C}$, ovvero i limiti inversi di sistemi inversi di $\mathcal{C}$-gruppi, dove $\mathcal{C}$ è una classe di gruppi finiti chiusa per immagini isomorfe. In particolare vengono studiati i gruppi profiniti, cioè gruppi pro-$\mathcal{C}$ dove $\mathcal{C}$ è la classe di tutti i gruppi finiti. Una delle proprietà più interessanti di un gruppo profinito deriva dalla sua struttura di gruppo topologico, risulta infatti che i gruppi profiniti sono tutti e soli i gruppi topologici quasi compatti e totalmente disconnessi.

Nel quinto capitolo vengono studiati i completamenti di un gruppo rispetto ad una base filtro non vuota di sottogruppi normali del gruppo di indice finito. In particolare si osserva che il completamento pro-p dell'insieme degli interi, cioè il completamento rispetto alla famiglia di tutti i sottogruppi di indice una potenza di un primo p, è costituito dall'insieme degli interi p-adici con la mappa di inclusione dagli interi agli interi p-adici. In questo capitolo alcune proprietà già dimostrate nella tesi di laurea triennale vengono dimostrate nuovamente tramite le proprietà dei limiti inversi.

L'interesse della comunità matematica verso lo studio dei gruppi profiniti nacque inizialmente dalla studio dei gruppi di Galois di estensioni di campi di Galois di grado infinito. Non a caso in un un primo momento i gruppi profiniti vennero chiamati 'gruppi di tipo Galois'. Il sesto capitolo tratta appunto delle estensioni di Galois di grado infinito in relazione con i gruppi profiniti. Viene esteso il Teorema di Corrispondenza di Galois nel caso di estensioni di Galois di grado infinito. Viene inoltre dimostrato che ogni gruppo di Galois è un gruppo profinito e che ogni gruppo profinito è isomorfo ad un gruppo di

Galois. Nell'appendice è presente un esempio di corrispondenza fra un gruppo di Galois ed un gruppo profinito a me ormai caro.

Notazioni

Data una famiglia di spazi topologici $(X_i, \tau_i)_{i \in I}$, il prodotto cartesiano delle X_i verrà indicato con $\prod_i X_i$ oppure con $\prod_{i \in I} X_i$, con $\mathcal{P}$ si indicherà la topologia prodotto nel prodotto cartesiano delle X_i.
Dato uno spazio topologico (X, τ), se Y è un sottoinsieme di X la topologia indotta su Y verrà indicata con $\mathcal{I}$ oppure con $\mathcal{I}_X$.
Dato uno spazio topologico (X, τ) e $\sim$ una relazione di equivalenza su X, la topologia quoziente su $X/\sim$ verrà indicata con $\mathcal{Q}$.
Se $f : X \longrightarrow Y$ è una applicazione fra insiemi biunivoca verrà indicata con f^{-1} l'applicazione inversa avente dominio Y e codominio X. Se $f : X \longrightarrow Y$ è una applicazione fra insiemi e B è un sottoinsieme di Y verrà indicato con $f^{-1}(B)$ l'insieme delle $x \in X$ tali che $f(x) \in B$.
Uno spazio topologico (X, τ) verrà chiamato quasi compatto se da ogni ricoprimento di aperti di X è possibile estrarre un sottoricoprimento di aperti finito, ovvero se vale la seguente proprietà: se $X = \bigcup_{i \in I} A_i$ con A_i aperti di X e I una famiglia di indici, allora esistono $n \in \mathbb{N}$ e $A_{i_1}, \ldots, A_{i_n}$ tali che $X = A_{i_1} \cup \ldots \cup A_{i_n}$.
Se G è un gruppo, g un elemento di G e H un sottoinsieme di G allora l'insieme $\{x \in G$ tale che esite $h \in H$ per cui $x = gh\}$ verrà denotato con gH; analogamente con Hg si intenderà l'insieme $\{x \in G$ tale che esite $h \in H$ per cui $x = hg\}$. Con H^{-1} si denoterà invece $\{h^{-1}$ con $h \in H\}$. Se K è un altro sottoinsieme di G per HK si intenderà l'insieme $\{hk$ tali che $h \in H$ e $k \in K\}$.
Se G è un gruppo topologico e H, N sono sottoinsiemi di G, con $H \leq G$ si intenderà che H è un sottogruppo chiuso di G, mentre con $N \triangleleft_O G$ si intenderà che N è un sottogruppo normale aperto di G.
Se X è un insieme si indicherà con id_X l'applicazione identica di X in se stesso.
L'insieme vuoto verrà indicato con $\emptyset$.
Se X è uno spazio topologico e A è un sottoinsieme di X la chiusura di A verrà indicata con $\overline{A}$.
Con $\mathbb{N}$ verrà indicato l'insieme dei numeri interi maggiori di 0.
Se i ed n sono due numeri interi positivi il massimo comun divisore fra i ed n verrà indicato con (i, n).

Capitolo 1

Spazi topologici

Definizione 1.1. Uno spazio topologico (X, τ) è detto totalmente disconnesso se i suoi unici sottospazi connessi diversi dall'insieme vuoto sono i singoli elementi di X, ovvero se vale la seguente proprietà: se Z è un sottoinsieme di X non vuoto tale che $(Z, \mathfrak{I})$ è connesso, allora esiste $x \in X$ tale che $Z = \{x\}$.
Si noti che $\{x\}$ è sempre connesso per ogni $x \in X$.

Osservazione 1.1. *Sia (X, τ) uno spazio topologico totalmente disconnesso, se Y è un sottoinsieme di X, allora $(Y, \mathfrak{I})$ è totalmente disconnesso.*

Dimostrazione. Sia Y_1 un sottoinsieme non vuoto di Y tale che $(Y_1, \mathfrak{I}_Y)$ è connesso, allora non esistono due aperti di $\mathfrak{I}_Y$ diversi dall'insieme vuoto e da Y_1, della forma $Y_1 \cap (A \cap Y)$ e $Y_1 \cap (B \cap Y)$ con A, B aperti di X tali che

$$(Y_1 \cap (A \cap Y)) \cup (Y_1 \cap (B \cap Y)) = Y_1$$

e

$$(Y_1 \cap (A \cap Y)) \cap (Y_1 \cap (B \cap Y)) = \emptyset.$$

Vogliamo dimostrare che Y_1 è uguale ad un solo elemento di Y.
Quanto affermato sopra è equivalente a dire che non esistono $A \cap Y_1$, $B \cap Y_1$ diversi dall'insieme vuoto e da Y_1 con A e B aperti di X tali che

$$(Y_1 \cap A) \cup (Y_1 \cap B) = Y_1$$

e

$$(Y_1 \cap A) \cap (Y_1 \cap B) = \emptyset.$$

Allora $(Y_1, \mathfrak{I}_X)$ è connesso, dunque esiste $x \in X$ tale che $Y_1 = \{x\}$, ma necessariamente $x \in Y$ dato che $Y_1 \subseteq Y$.

□

Osservazione 1.2. *Se (X_i, τ_i) sono spazi topologici totalmente disconnessi per ogni $i \in I$, allora lo spazio topologico $(\prod_{i\in I} X_i, \mathcal{P})$ è totalmente disconnesso.*

Dimostrazione. Sia $Z \subseteq \prod_i X_i$, con Z connesso rispetto la topologia indotta. Per definizione di topologia prodotto la proiezione

$$\begin{array}{rccc} p_j : (\prod_{i\in I} X_i, \mathcal{P}) & \longrightarrow & (X_j, \tau_j) \\ (x_i)_{i\in I} & \longmapsto & x_j \end{array}$$

è continua per ogni $j \in I$, allora anche la restrizione $p_{j_{|Z}} : (Z, \mathcal{I}_{\prod X_i}) \longrightarrow (X_j, \tau_j)$ è continua per ogni j.
Poiché l'immagine di uno sapzio connesso tramite una applicazione continua è connessa $p_{j_{|Z}}(Z)$ è connesso per $\mathcal{I}_{X_j}$, allora $p_{j_{|Z}}(Z)$ è un punto per ogni j, quindi Z contiene al più un punto e così si ha che $(\prod_{i\in I} X_i, \mathcal{P})$ è totalmente disconnesso.

□

Osservazione 1.3. *Se $f : X \longrightarrow Y$ è un omeomorfismo fra spazi topologici e X è totalmente disconnesso, allora Y è totalmente disconnesso.*

Dimostrazione. Sia Y_1 un sottoinsieme di Y tale che $(Y_1, \mathcal{I}_Y)$ sia connesso. La funzione $f^{-1} : Y \longrightarrow X$ è continua dunque $(f^{-1}(Y_1), \mathcal{I}_X)$ è connesso, allora $f^{-1}(Y_1)$ è al più un punto e quindi, essendo la f biunivoca, anche Y_1 è al più un punto. Dunque Y è totalmente disconnesso.

□

Lemma 1.4. *Sia X uno spazio topologico quasi compatto e di Hausdorff,*

1. *se C, D sono due chiusi di X disgiunti, allora esistono U, V aperti di X tali che U contiene C, V contiene D e U, V sono ancora disgiunti.*

2. *Se x è un elemento di X e se si pone*

$$A := \bigcap \{S \text{ tale che } S \text{ aperto e chiuso di } X \text{ e } x \in S\},$$

   si ha che A è connesso.

3. *Se X è anche totalmente disconnesso allora per ogni U aperto di X esistono B_i aperti e chiusi di X tali che $U = \bigcup_{i\in I} B_i$, in altre parole, esiste una base di aperti e chiusi per la topologia di X.*

Dimostrazione. 1. Dimostriamo prima che per ogni $c \in C$ esistono U_c intorno aperto di c in X e V_c aperto di X contenente D, con U_c e V_c disgiunti.
Sia $c \in C$ fissato, allora per ogni $d \in D$ esistono O_d intorno aperto di c in X, P_d intorno aperto di d in X con O_d e P_d disgiunti, poiché $c, d \in X$ che è di Haudorff.
Si ha che $X = (X \setminus D) \cup (\bigcup_{d \in D} P_d)$ allora, poiché D è un chiuso di X, poiché P_d è aperto per ogni d e poiché X è quasi compatto, esistono $m \in \mathbb{N}$ e $d_1, \ldots, d_m \in D$ tali che $X = (X \setminus D) \cup P_{d_1} \cup \ldots \cup P_{d_m}$ (si noti che se non è presente $(X \setminus D)$ nella sottofamiglia finita estratta si può sempre aggiungere).
Sia $V_c := P_{d_1} \cup \ldots \cup P_{d_m}$ e $U_c := O_{d_1} \cap \ldots \cap O_{d_m}$.
Chiaramente U_c e V_c sono aperti. Si ha che $U_c \cap V_c = \emptyset$: se $x \in V_c$ allora esiste $i \in \{1, \ldots, m\}$ tale che $x \in P_{d_i}$, ma $P_{d_i} \cap O_{d_i} = \emptyset$ allora x non appartiene a O_{d_i} e quindi x non appartiene a $O_{d_1} \cap \ldots \cap O_{d_m} = U_c$.
Si ha che $c \in U_c$ poiché $c \in O_{d_i}$ per ogni i. Inoltre $D \subseteq V_c$ poiché $D \subseteq X$ e $X = (X \setminus D) \cup V_c$.
Dimostriamo ora la tesi del lemma.
Si ha che $X = (X \setminus C) \cup (\bigcup_{c \in C} U_c)$. Allora, poiché C è un chiuso di X, poiché gli U_c sono aperti per ogni c e poiché X è quasi compatto, esistono $n \in \mathbb{N}$ e $c_1, \ldots, c_n \in C$ tali che $X = (X \setminus C) \cup U_{c_1} \cup \ldots \cup U_{c_n}$. Siano $U := U_{c_1} \cup \ldots \cup U_{c_n}$ e $V := V_{c_1} \cap \ldots \cap V_{c_n}$.
Chiaramente U e V sono aperti. Si ha che $U \cap V = \emptyset$: se $x \in U$ allora esiste $i \in \{1, \ldots, n\}$ tale che tale che $x \in U_{c_i}$, quindi x non appartiene a V_{c_i}, dato che $U_{c_i} \cap V_{c_i}$ è uguale all'insieme vuoto, allora x non appartiene a $V_{c_1} \cap \ldots \cap V_{c_n} = V$.
Inoltre U contiene C poiché $C \subseteq X = (X \setminus C) \cup U$.
Si ha anche che V contiene D poiché V_{c_i} contiene D per ogni i.

2. Supponiamo che per assurdo esistano C, D, diversi da A e dall'insieme vuoto, aperti in A per la topologia indotta da X, con C e D disgiunti tali che $C \cup D = A$. Gli insiemi C e D sono anche chiusi in A poiché $A \setminus C = D$ è aperto di A e allo stesso modo $A \setminus D = C$. Si ha che A è chiuso in X poiché è intersezione di chiusi allora C, essendo un chiuso per la topologia indotta da X, è anche un chiuso di X (esiste C' chiuso di X tale che C è uguale ad $A \cap C'$). Allo stesso modo D è un chiuso di X. Si ha quindi che C e D sono due chiusi di X disgiunti, allora per il precedente punto di questo lemma esistono un aperto U di X contenente C ed un aperto V di X contenente D, con U e V disgiunti.
Sia $B := X \setminus (U \cup V)$. Si ha che B è un chiuso di X poiché U e V sono aperti di X. Si ha che $B \cap (\bigcap_{x \in S} \{S \text{ t.c. } S \text{ aperto e chiuso di } X\})$ è uguale all'insieme vuoto poiché $A = C \cup D \subseteq U \cup V$. Poiché X è quasi compatto esistono $n \in \mathbb{N}$ e $S_{i_1}, \ldots, S_{i_n}$ tali che $B \cap S_{i_1} \cap \ldots \cap S_{i_n}$ è uguale all'insieme vuoto (si noti che se B non fa parte della sottofamiglia finita estratta vi si può sempre inserire).

Sia $I := S_{i_1} \cap \ldots \cap S_{i_n}$, si ha che $I \subseteq U \cup V$: se $x \in S_{i_r}$ per ogni r allora x non può appartenere a B, ma $B = X \setminus (U \cup V)$ e quindi x appartiene a $U \cup V$, dunque $\bigcap_{r=1}^{n} S_{i_r} \subseteq U \cup V$.
Allora $I = I \cap (U \cup V) = (I \cap U) \cup (I \cap V)$ e $(I \cap U) \cap (I \cap V) = \emptyset$ poiché U e V sono insiemi disgiunti. $I \cap U$ è aperto in I per la topologia indotta da X e lo stesso vale per $I \cap V$. Si ha anche che $I \cap U$ è chiuso in I per la topologia indotta da X, poiché $I \setminus (I \cap U) = I \cap V$ è un aperto di I. Allo stesso modo $I \cap V$ è chiuso in I per la topologia indotta da X.
Dunque, poiché I è aperto e chiuso in X si ha che $I \cap U$ e $I \cap V$ sono aperti e chiusi in X.
Sia $x \in I$, poiché $I = (I \cap U) \cup (I \cap V)$ e $I \cap U$ è disgiunto da $I \cap V$, o $x \in I \cap U$ oppure $x \in I \cap V$.
Possiamo supporre che $x \in I \cap U$. Allora, essendo $I \cap U$ un aperto e chiuso di X contenente x, si ha che $A \subseteq I \cap U$. Poiché $D \subseteq A$ e $D \subseteq V$, si ha che $D \subseteq A \cap V \subseteq (I \cap U) \cap V = \emptyset$ dunque l'insieme D sarebbe uguale al vuoto che è assurdo.

3. Sia U un aperto di X, fissiamo un elemento x di U.
Dimostriamo che per ogni $y \in X$ con y diverso da x, esiste F_y aperto e chiuso di X tale che $x \in F_y$ ma $y \notin F_y$. Fissato un $y \in X$, y diverso da x, supponiamo per assurdo che per ogni F_y contenente x con F_y aperto e chiuso di X, anche $y \in F_y$. Allora $y \in \bigcap_{x \in S} \{S \text{ t.c. } S \text{ aperto e chiuso di } X\}$ che per il precedente punto è un connesso, quindi, essendo X totalmente disconnesso, avremmo $y = x$ che è assurdo.
Tenendo ancora fissato $x \in U$, si ha che $X = U \cup (\bigcup_{y \in X \setminus \{x\}} (X \setminus F_y))$ dunque, essendo X quasi compatto, esistono un intero positivo n e $y_1 \ldots y_n \in X$ tali che $X = U \cup (X \setminus F_{y_1}) \cup \ldots \cup (X \setminus F_{y_n})$.
L'insieme $F_{y_1} \cap \ldots \cap F_{y_n}$ è contenuto in U poiché se $z \in F_{y_1} \cap \ldots \cap F_{y_n}$ allora $z \notin X \setminus F_{y_i}$ per ogni i quindi $z \in U$. Definiamo l'insieme $C_x := F_{y_1} \cap \ldots \cap F_{y_n}$. Abbiamo che $x \in C_x$ e C_x è un aperto e chiuso di X. Inoltre si ha che $U = \bigcup_{x \in U} C_x$.

□

Lemma 1.5. *Sia X uno spazio topologico totalmente disconnesso, allora $\{x\}$ è un chiuso di X per ogni $x \in X$.*

Dimostrazione. Definiamo $C := \overline{\{x\}}$, chiaramente C è un chiuso di X. Basta dimostrare che C è connesso perché in tal caso si avrebbe che $C = \overline{\{x\}} = \{x\}$ e quindi $\{x\}$ è un chiuso di X. Se per assurdo C non è conneso allora esistono A e B aperti di C per la

topologia indotta da X, con A e B disgiunti, diversi dall'insieme vuoto e da C tali che $C = A \cup B$. Possiamo supporre che $x \in A$ e quindi $x \notin B$. Si ha che A è anche chiuso in C per la topologia indotta da X poiché $C \setminus A = B$ aperto di C, allora A è chiuso anche in X essendo C chiuso in X. Però $\{x\} \subseteq A$ quindi $C = \overline{\{x\}} \subseteq \overline{A} = A \subseteq C$ allora $A = C$ che è assurdo.

□

Capitolo 2

Gruppi topologici

Definizione 2.1. Sia $(G, \cdot, \tau)$ un gruppo per l'operazione $\cdot$ ed uno spazio topologico per la topologia τ. G è gruppo topologico se l'applicazione

$$\begin{array}{ccc} \chi : (G \times G, \mathcal{P}) & \longrightarrow & (G, \tau) \\ (g_1, g_2) & \longmapsto & g_1 \cdot g_2^{-1} \end{array}$$

con $\mathcal{P}$ la topologia prodotto, è continua.

Osservazione 2.1. *Sia $(G, \cdot, \tau)$ un gruppo ed uno spazio topologico.*

1. *Se*
$$\begin{array}{ccc} \psi : G & \longrightarrow & G \\ g & \longmapsto & g^{-1} \end{array} , \quad \begin{array}{ccc} \chi : G \times G & \longrightarrow & G \\ (g_1, g_2) & \longmapsto & g_1 g_2 \end{array}$$
sono continue allora G è un gruppo topologico.

2. *Se H è un sottogruppo di G ed H è munito della topologia indotta, allora H è un gruppo topologico.*

3. *Siano $(G_i, \cdot_i, \tau_i)$ dei gruppi topologici, allora lo spazio topologico $(\prod_i G_i, \cdot, \mathcal{P})$, dove $\cdot$ è l'operazione definita componente per componente, e $\mathcal{P}$ è la topologia prodotto, è un gruppo topologico.*

Dimostrazione. Le dimostrazioni di questi tre punti sono simili ed elementari, dimostriamo ad esempio il punto 3.
Basta dimostrare che la mappa

$$\begin{array}{ccc} \prod_i X_i \times \prod_i X_i & \longrightarrow & X_j \\ (x_i)_{i \in I}, (y_i)_{i \in I} & \longmapsto & x_j \cdot y_j^{-1} \end{array}$$

è continua per ogni j (poiché una mappa f che va da uno spazio topologico ad un prodotto cartesiano munito della topologia prodotto è continua se e solo se lo sono tutte le mappe ottenute componendo f con le proiezioni).
Definiamo la seguente composizione di mappe

$$\begin{array}{rccccc} \theta_j : \prod_i X_i \times \prod_i X_i & \longrightarrow & \prod_i X_i & \longrightarrow & X_j \\ (x_i)_{i\in I}, (y_i)_{i\in I} & \longmapsto & (x_i)_{i\in I} & \longmapsto & x_j \end{array}$$

che è continua per ogni j per definizione di topologia prodotto.
Definiamo la seguente composizione di mappe

$$\begin{array}{rccccc} \varphi_j : \prod_i X_i \times \prod_i X_i & \longrightarrow & X_j & \longrightarrow & X_j \\ (x_i)_{i\in I}, (y_i)_{i\in I} & \longmapsto & y_j & \longmapsto & y_j^{-1} \end{array}$$

che è continua per ogni j per definizione di topologia prodotto e poiché X_j è un gruppo topologico per ogni j.
Allora

$$\begin{array}{rcc} \prod_i X_i \times \prod_i X_i & \longrightarrow & X_j \times X_j \\ (x_i)_{i\in I}, (y_i)_{i\in I} & \longmapsto & \theta_j\left((x_i)_{i\in I}, (y_i)_{i\in I}\right), \varphi_j\left((x_i)_{i\in I}, (y_i)_{i\in I}\right) \end{array}$$

è continua per ogni j e quindi poiché X_j è un gruppo topologico per ogni j la seguente composizione di mappe è continua

$$\begin{array}{rccccc} \prod_i X_i \times \prod_i X_i & \longrightarrow & X_j \times X_j & \longrightarrow & X_j \\ (x_i)_{i\in I}, (y_i)_{i\in I} & \longmapsto & x_j, y_j^{-1} & \longmapsto & x_j \cdot y_j^{-1}. \end{array}$$

□

Osservazione 2.2. *Sia $(G, \cdot, \tau)$ un gruppo topologico.*

a) *1. La mappa*

$$\begin{array}{rcc} G \times G & \longrightarrow & G \\ x, y & \longmapsto & x \cdot y \end{array}$$

è continua.
La mappa

$$\begin{array}{rcc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array}$$

è un omeomorfismo.

2. *Se g è un elemento di G allora la mappa*

$$\begin{array}{rccc} \psi_g : & G & \longrightarrow & G \\ & x & \longmapsto & gx \end{array}$$

e la mappa

$$\begin{array}{rccc} \psi'_g : & G & \longrightarrow & G \\ & x & \longmapsto & xg \end{array}$$

sono omemorfismi.

b) 1. *Se H è un insieme aperto di G e g è un elemento di G allora Hg e gH sono aperti di G;*

2. *se H è un sottogruppo chiuso di G e g è un elemento di G allora Hg e gH sono chiusi di G.*

c) 1. *Ogni sottogruppo aperto di G è chiuso.*

2. *Ogni sottogruppo chiuso di G di indice finito è aperto.*

3. *Se G è quasi compatto allora ogni sottogruppo aperto di G ha indice finito.*

d) *Se H è un sottogruppo di G e H contiene U, dove U è un aperto di G diverso dall'insieme vuoto, allora anche H è un aperto di G.*

e) *Se K è un sottogruppo normale di G allora*

1. *la mappa quoziente $q : G \longrightarrow G/K$ è una mappa fra spazi topologici aperta,*

2. *G/K è un gruppo topologico per la topologia quoziente.*

f) 1. *G è di Hausdorff se e solo se $\{1_G\}$ è un chiuso di G,*

2. *se K è un sottogruppo normale di G allora G/K è di Hausdorff se e solo se K è chiuso in G,*

3. *se G è totalmente disconnesso allora G è di Hausdorff.*

Il seguente punto ci tornerà molto utile poiché se C è un aperto allora CS è un aperto per ogni sottoinsieme S di G, mentre se C è un chiuso e S è un sottoinsieme di G non è detto che CS sia un chiuso.

g) Se G è quasi compatto e di Hausdorff, C, D sono due chiusi di G allora CD è un chiuso di G.

h) Se G è quasi compatto, Y è un chiuso di G e $(X_\lambda)_{\lambda\in\Lambda}$ è una famiglia di chiusi di G tali che per ogni λ_1, $\lambda_2 \in \Lambda$ esiste $\mu \in \Lambda$ tale che $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$, allora $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda}(X_\lambda Y)$.

Dimostrazione. a) La dimostrazione è simile a quella dell'Osservazione 2.1. Per il punto 1 è sufficiente considerare le mappe continue

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & 1_G \end{array} \qquad \text{e} \qquad \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x. \end{array}$$

Per il punto 2 invece si possono considerare ad esempio le mappe continue

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x \end{array} \qquad \text{e} \qquad \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1}. \end{array}$$

b) Per il punto a) per ogni elemento g di G la mappa ψ_g è un omeomorfismo quindi ψ_g è aperta per ogni g. Dunque se H è un aperto di G l'insieme $\psi_g(H)$ è un aperto di G per ogni g, ma $\psi_g(H) = \{\psi_g(h) \text{ tale che } h \in H\} = gH$. Analogamente per ogni g si dimostra che Hg è aperto e che gH, Hg sono chiusi se H è chiuso.

c) Sia H un sottogruppo di G. Si verifica facilmente che $G \setminus H = \bigcup_{g \in G \setminus H} Hg$.

1. Se H è aperto allora Hg è aperto per ogni $g \in G \setminus H$, quindi $G \setminus H$ è aperto. Dunque H è chiuso.
2. Se H ha indice finito allora esistono $n \in \mathbb{N}$ e $g_1, \ldots, g_n \in G \setminus H$ tali che $G \setminus H = Hg_1 \cup \ldots \cup Hg_n$. Se H è chiuso anche $G \setminus H$ è chiuso, poiché unione finita di chiusi, dunque H è aperto.
3. Se G è quasi compatto e H è aperto, allora per ogni $g \in G \setminus H$ si ha che Hg è aperto, quindi esistono un intero positivo n e $g_1, \ldots, g_n \in G \setminus H$ tali che $G \setminus H = Hg_1 \cup \ldots \cup Hg_n$. Si ha dunque che H ha indice finito.

d) Per il punto b) di questa osservazione Uh è un aperto di G, ma $H = \bigcup_{h \in H} Uh$ poiché $Uh \subseteq H$ per ogni $h \in H$ e se h è un elemento di H e u un elemento di U allora $u^{-1}h \in H$ e $h = u(u^{-1}h)$. Dunque anche H è un aperto di G.

e) 1. Sia V un aperto di G allora $KV = \bigcup_{k \in K} kV$ è un aperto di G. Per definizione $q(V)$ è un aperto per la topologia quoziente se e solo se $q^{-1}(q(V))$ è un aperto di G, ma $q^{-1}(q(V)) = KV$.

2. Poiché K è normale già sappiamo che G/K è un gruppo. Si ha che G/K è un gruppo topologico se la mappa

$$\begin{array}{rccc} m: & G/K \times G/K & \longrightarrow & G/K \\ & (g_1K, g_2K) & \longmapsto & g_1 \cdot g_2^{-1}K \end{array}$$

è continua.
Sia (g_1K, g_2K) un generico elemento di $G/K \times G/K$ e sia V un aperto di

G/K con $m(g_1K, g_2K) \in V$, vogliamo trovare un aperto A di $G/K \times G/K$ con $(g_1K, g_2K) \in A$ tale che $m(A) \subseteq V$.
Poiché G è un gruppo topologico la mappa ψ che ad ogni $(g_1, g_2) \in G \times G$ associa $g_1 g_2^{-1} \in G$ è continua e poiché q è continua la mappa $q \circ \psi$ è continua. Esiste quindi un aperto B di $G \times G$ con $(g_1, g_2) \in B$ tale che $q \circ \psi(B) \subseteq V$. Per definizione della topologia prodotto $B = \bigcup_{i \in I} W_1^i \times W_2^i$ con W_1^i e W_2^i aperti di G per ogni $i \in I$. Sia k tale che $(g_1, g_2) \in W_1^k \times W_2^k$. L'insieme $q \circ \psi(W_1^k \times W_2^k)$ è contenuto in V.
Prendiamo $A = q(W_1^k) \times q(W_2^k)$. Poiché q è aperta si ha che A è un aperto di $G/K \times G/K$ contenente (g_1K, g_2K). Proviamo che $m(q(W_1^k) \times q(W_2^k))$ è contenuto in V. Se $z \in m(q(W_1^k) \times q(W_2^k))$ esistono $w_1, w_2 \in W_1^k \times W_2^k$ tali che $z = m(w_1K, w_2K)$, ma $m(w_1K, w_2K) = w_1 w_2^{-1} K = q \circ \psi(w_1, w_2) \in V$.

f) 1. Se G è di Hausdorff $G \setminus \{1_G\}$ è un aperto dato che per ogni $y \in G \setminus \{1_G\}$ esiste un intorno di y contenuto in $G \setminus \{x\}$.
Viceversa supponiamo che $\{1_G\}$ sia un chiuso di G. Siano a e b due elementi di G distinti. Troviamo due aperti di G disgiunti tali che uno contenga a e l'altro contenga b.
Si ha che $\psi_{a^{-1}}(1_G) = a^{-1}$, quindi a^{-1} è un chiuso essendo $\psi_{a^{-1}}$ un omeomorfismo per il punto 1 di questa proposizione. Per lo stesso motivo $\psi_b(a^{-1}) = a^{-1}b$ è un chiuso e quindi $U := G \setminus \{a^{-1}b\}$ è un aperto in G contenente 1_G, ma non contenente $a^{-1}b$ (poiché $a^{-1}b = 1_G$ se e solo se $a = b$).
Essendo G un gruppo topologico la mappa χ che ad ogni $(g_1, g_2) \in G \times G$ associa $g_1 g_2^{-1} \in G$ è continua, esiste allora un aperto A di $G \times G$ contenente $(1_G, 1_G)$ tale che $\chi(A) \subseteq U$.
Per un ragionamento analogo a quello fatto nel precedente punto di questa dimostrazione possiamo supporre che $A = V \times W$ con V e W aperti di G contenenti entrambi 1_G. Proviamo che aV e bW sono due aperti disgiunti, con aV contenente a e bV contenente b, concludendo così la dimostrazione.
Si ha che $\chi(A) = VW^{-1} \subseteq U$ e quindi $a^{-1}b$ non appartiene a VW^{-1}. Allora $aV \cap bW = \emptyset$ infatti se esistessero $v \in V$ e $w \in W$ tali che $av = bw$ si avrebbe che $vw^{-1} = a^{-1}b$ e quindi $a^{-1}b$ sarebbe contenuto in VW^{-1}, che è assurdo. Poiché 1_G appartiene sia a V che a W si ha che $a \in aV$ e $b \in bW$ e dato che V e W sono aperti anche aV e bW sono aperti.

2. Per il precedente punto G/K è di Hausdorff se e solo se $1_{G/K}$ è un chiuso di G/K se e solo se, per definizione di topologia quoziente, $\pi^{-1}(1_{G/K}) = K$ è un chiuso di G, dove π è la mappa quoziente.

3. Se G è totalmente disconnesso allora per il Lemma 1.5 $\{1_G\}$ è un chiuso di G quindi per il punto f) di questa osservazione G è di Hausdorff.

g) Sia χ la mappa che ad ogni $(g_1, g_2) \in G \times G$ associa $g_1 \cdot g_2^{-1} \in G$. La mappa χ è continua per definizione di gruppo topologico.
Si ha che C e D sono quasi compatti per la topologia indotta da G poiché C e D sono chiusi e poiché G è quasi compatto. Allora $(C \times D, \mathcal{P})$ è quasi compatto per il teorema di Tychoff. Ma $(C \times D, \mathcal{P}) = (C \times D, \mathcal{I}_{G\times G})$[1], dunque anche con la topologia indotta da $G \times G$ lo spazio $C \times D$ è quasi compatto. La mappa $\chi_{|C\times D}$ è continua, dunque $\chi_{|C\times D}(C \times D)$ è quasi compatto in G. Però G è di Hausdorff allora $\chi_{|C\times D}(C \times D) = CD$ è chiuso.

h) Proviamo la doppia inclusione.
Chiaramente $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y \subseteq \bigcap_{\lambda\in\Lambda}(X_\lambda Y)$.
Dimostriamo ora che $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y \supseteq \bigcap_{\lambda\in\Lambda}(X_\lambda Y)$.

Facciamo vedere che se $g \in G$ non appartiene a $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y$ allora esiste $\mu \in \Lambda$ tale che g non appartiene a $X_\mu Y$. Si ha che $gY^{-1} \cap (\bigcap_{\lambda\in\Lambda} X_\lambda)$ è uguale all'insieme vuoto infatti se esistesse $y \in Y$ tale che $gy^{-1} \in \bigcap_{\lambda\in\Lambda} X_\lambda$ allora g apparterrebbe a $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y$. Si ha che Y^{-1} è un chiuso di G poiché Y è un chiuso per ipotesi e poiché l'applicazione che manda un elemento di g nel suo inverso è un omeomorfismo e quindi è chiusa. Ma anche gli X_λ sono chiusi allora essendo G quasi compatto esistono $n \in \mathbb{N}$ e $X_{\lambda_1}, \ldots, X_{\lambda_n}$ tali che $gY^{-1} \cap X_{\lambda_1} \cap \ldots \cap X_{\lambda_n} = \emptyset$. Per ipotesi esiste $\mu \in \Lambda$ tale che $X_\mu \subseteq X_{\lambda_1} \cap \ldots \cap X_{\lambda_n}$, poiché abbiamo un numero finito di X_λ. Allora $gY^{-1} \cap X_\mu = \emptyset$ e quindi g non appartiene a $X_\mu Y$, come volevamo inizialmente dimostrare.

□

Esempio 1. *Esistono dei sottogruppi di un gruppo topologico che non sono né chiusi né aperti.*

Dimostrazione. Sia $(\mathbb{R}, \cdot, \mathcal{E})$ l'insieme dei numeri reali munito del prodotto e della topologia euclidea. Chiaramente $(\mathbb{R}, \cdot, \mathcal{E})$ è un gruppo topologico e $\mathbb{Q}$ è un suo sottogruppo. Se per assurdo $\mathbb{Q}$ fosse chiuso in $\mathbb{R}$, allora $\mathbb{R} \setminus \mathbb{Q}$ sarebbe un aperto di $\mathbb{R}$. Quindi per ogni $z \in \mathbb{R} \setminus \mathbb{Q}$ esisterebbe un intervallo aperto $]a, b[$ contenente z tale che $]a, b[\subseteq \mathbb{R} \setminus \mathbb{Q}$ che è assurdo.

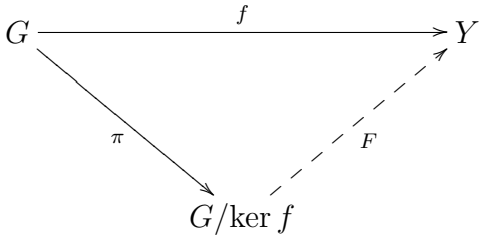
□

Occupiamoci ora dei tre teoremi di isomorfismo nel caso di gruppi topologici.

[1] Se si vuole dimostrare questo fatto si provi che le due topologie hanno una stessa base.

Definizione 2.2. Siano G e G' due gruppi topologici, una mappa da G a G' è detta isomorfismo di gruppi topologici se è un isomorfismo di gruppi, è continua e la sua inversa è continua.
Due gruppi topologici si dicono isomorfi come gruppi topologici se esiste un isomorfismo di gruppi topologici fra i due.

Teorema 2.3 (Primo teorema di isomorfismo per gruppi topologici)**.** *Siano G e Y due gruppi topologici. Sia $f : G \longrightarrow Y$ un omomorfismo di gruppi continuo e $\pi : G \longrightarrow G/\ker f$ la mappa quoziente, allora esiste ed è unico un omomorfismo di gruppi continuo $F : G \longrightarrow Y$ tale che $f = F \circ \pi$, ovvero tale che il seguente diagramma sia commutativo.*



Se inoltre abbiamo che f è suriettiva e che vale una fra le seguenti due ipotesi

a) f è aperta,

b) G è quasi compatto e Y è di Hausdorff

allora F è un isomorfismo di gruppi topologici.

Dimostrazione. Definiamo

$$\begin{array}{rccc} F: & G/\ker f & \longrightarrow & Y \\ & g\ker f & \longmapsto & f(g). \end{array}$$

La mappa F è l'unico omomorfismo di gruppi tale che $f = F \circ \pi$ ed è chiaramente iniettiva, inoltre F è continua poiché f è continua.
Se f è suriettiva allora $Y = f(G)$ e quindi F è suriettiva.

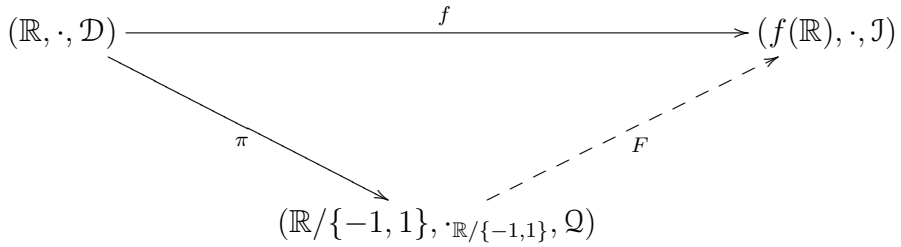
a) Dimostriamo che F^{-1} è continua cioè che per ogni B aperto per la topologia quoziente di $G/\ker f$ si ha che $F(B)$ è un aperto di Y. Sia $A := \pi^{-1}(B)$, che per definizione di topologia quoziente è aperto. Essendo π suriettiva, abbiamo che $B = \pi(\pi^{-1}(B))$ che è uguale a $\pi(A)$. Si ha allora che $F(B) = F \circ \pi(A) = f(A)$, ma $f(A)$ è un aperto di Y poiché f è aperta.

b) Se G è quasi compatto anche $G/\ker f$ è quasi compatto essendo π continua e suriettiva. Poiché F è una mappa continua e biunivoca da uno spazio quasi compatto ad uno spazio di Hausdorff allora F è anche un omeomorfismo.

□

Esempio 2. *Mostriamo che con le sole ipotesi che la mappa f sia un omomorfismo di gruppi continuo suriettivo la seconda parte del teorema non è verificata.*

Dimostrazione. Sia $(\mathbb{R}, \cdot, \mathcal{D})$ l'insieme dei numeri reali munito del prodotto e della topologia discreta. Sia $(\mathbb{R}, \cdot, \mathcal{E})$ l'insieme dei numeri reali munito del prodotto e della topologia euclidea. Chiaramente $(\mathbb{R}, \cdot, \mathcal{D})$ e $(\mathbb{R}, \cdot, \mathcal{E})$ sono due gruppi topologici. Consideriamo la mappa f che va da $(\mathbb{R}, \cdot, \mathcal{D})$ a $(\mathbb{R}, \cdot, \mathcal{E})$ e che ad ogni x associa x^2. La mappa f è chiaramente un omomorfismo di gruppi continuo. Inoltre $\ker f = \{-1, 1\}$. Consideriamo il seguente diagramma commutativo.



Si noti che $(\mathbb{R}/\{-1, 1\}, \mathcal{Q}) = (\mathbb{R}/\{-1, 1\}, \mathcal{D})$. Chiaramente $(\mathbb{R}/\{-1, 1\}, \mathcal{Q})$ è totalmente disconnesso. Se per assurdo F fosse un isomorfismo di gruppi topologici per l'Osservazione 1.3 si avrebbe che anche $f(\mathbb{R})$ sarebbe totalmente disconnesso. Questo è assurdo poiché ad esempio l'intervallo $]3, 5[$ è un insieme connesso di $f(\mathbb{R})$.

□

Teorema 2.4 (Secondo teorema di isomorfismo per gruppi topologici)**.** *Siano H un sottogruppo di G ed N un sottogruppo normale di G, allora $N \cap H$ è un sottogruppo normale di H. Se H è quasi compatto e NH/N è di Hausdorff allora $H/(N \cap H)$ è isomorfo come gruppo topologico a NH/N.*

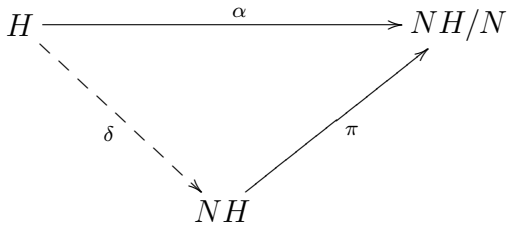
Dimostrazione. La mappa

$$\begin{array}{rccc} \alpha: & H & \longrightarrow & NH/N \\ & h & \longmapsto & hN \end{array}$$

è un omomorfismo di gruppi tale che $\ker \alpha = H \cap N$ (quindi si ha immediatamente che $N \cap H$ è un sottogruppo normale di H) e $f(G) = NH/N$.
Se proviamo che α è continua, per il primo teorema di isomorfismo per gruppi topologici abbiamo dimostrato il teorema. La mappa

$$\begin{array}{rccc} \delta: & (H, \mathcal{I}_G) & \longrightarrow & (NH, \mathcal{I}_G) \\ & h & \longmapsto & 1_G \cdot h \end{array}$$

è continua in quanto id_G è continua. Se π è la mappa quoziente da NH in NH/N si ha che $\pi \circ \delta$ è continua.
Vale che il seguente diagramma è commutativo.



Dunque essendo $\alpha = \pi \circ \delta$ si ha che α è continua.

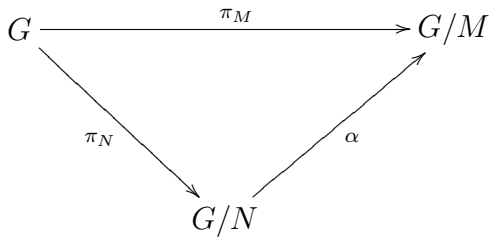
□

Teorema 2.5 (Terzo teorema di isomorfismo per gruppi topologici)**.** *Sia G un gruppo topologico, siano M ed N due sottogruppi normali di G con N sottogruppo di M.*
Allora M/N è un sottogruppo normale di G/N e $(G/N)/(M/N)$ è isomorfo a G/M come gruppo topologico.

Dimostrazione. Consideriamo la mappa

$$\begin{array}{rccc} \alpha: & G/N & \longrightarrow & G/M \\ & gN & \longmapsto & gM \end{array}$$

della quale è noto che è ben definita, che è un omomorfismo di gruppi, che è suriettiva e che $\ker \alpha = M/N$. Se dimostriamo che α è aperta, per il Teorema 2.3 la dimostrazione è conclusa.
Si ha chiaramente che $\pi_M = \alpha \circ \pi_N$.



Se B è un aperto di G/N allora, essendo π_N suriettiva, si ha che $B = \pi_N(\pi_N^{-1}(B))$ e $A := \pi_N^{-1}(B)$ è un aperto di G. Dunque $\alpha(B) = \alpha \circ \pi_N(A) = \pi_M(A)$ è un aperto di G/M poiché π_M è aperta per l'Osservazione 2.2 punto e).

□

Lemma 2.6. *Siano G e G' due gruppi topologici e sia $f : G \longrightarrow G'$ un isomorfismo di gruppi topologici. Sia C un sottogruppo normale di G. Allora $f(C)$ è un sottogruppo normale di G' e G/C è isomorfo come gruppo topologico a $G'/f(C)$.*

Dimostrazione. Poiché f è un isomorfismo di gruppi e C è un sottogruppo normale di G si ha che $f(C)$ è un sottogruppo normale di G'.
Consiederiamo la mappa

$$\begin{array}{rccc} \psi: & G/C & \longrightarrow & G'/f(C) \\ & gC & \longmapsto & f(g)f(C) \end{array}$$

che risulta chiaramente essere un isomorfismo di gruppi poiché f è un isomorfismo di gruppi.
Si ha inoltre che $\psi \circ \pi_C = \pi_{f(C)} \circ f$, ovvero che il seguente diagramma è commutativo.

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle \pi_C}\downarrow & & \downarrow{\scriptstyle \pi_{f(C)}} \\ G/C & \xrightarrow[\quad \psi \quad]{} & G'/f(C) \end{array}$$

Di conseguenza vale che $\pi_C \circ f^{-1} = \psi^{-1} \circ \pi_{f(C)}$.
Proviamo ora che ψ è continua. Sia V un aperto di $G'/f(C)$ vogliamo dimostrare che $\psi^{-1}(V)$ è un aperto di G/C cioè che, per definizione di topologia quoziente, ${\pi_C}^{-1}(\psi^{-1}(V))$ è un aperto di G. Ma

$${\pi_C}^{-1}(\psi^{-1}(V)) = (\psi \circ \pi_C)^{-1}(V) = (\pi_{f(C)} \circ f)^{-1}(V) = f^{-1}({\pi_{f(C)}}^{-1}(V))$$

che è aperto poiché f e $\pi_{f(C)}$ sono continue.
Proviamo ora che ψ^{-1} è continua. Sia U un aperto di G/C vogliamo dimostrare che $\psi(U)$ è un aperto di $G'/f(C)$ cioè che ${\pi_{f(C)}}^{-1}(\psi(U))$ è un aperto di G'. Si ha che

$${\pi_{f(C)}}^{-1}(\psi(U)) = (\psi^{-1} \circ \pi_{f(C)})^{-1}(U) = (\pi_C \circ f^{-1})^{-1}(U) = f({\pi_C}^{-1}(U))$$

che è aperto poiché f^{-1} e π_C sono continue.

□

Lemma 2.7. *Sia G un gruppo topologico quasi compatto, sia C un sottoinsieme di G chiuso e aperto con $1_G \in C$, allora C contiene un sottogruppo normale aperto di G.*

Dimostrazione. Per ogni $x \in C$ definiamo $W_x := Cx^{-1}$. Si ha che W_x è un aperto di G contenente 1_G. Chiaramente $W_x x \subseteq C$ per ogni x. Poiché la mappa ψ che ad ogni $(g_1, g_2) \in G \times G$ associa $g_1 g_2 \in G$ è continua esiste un aperto A di $G \times G$ contenente $(1_G, 1_G)$ tale che $\psi(A) \subseteq W_x$. Possiamo supporre che $A = L_x \times R_x$ dove L_x e R_x sono aperti di G entrambi contenenti 1_G. Dunque $L_x R_x = \psi(A) \subseteq W_x$.
Sia $S_x := L_x \cap R_x$. Si ha che $S_x S_x \subseteq W_x$ dato che $S_x S_x \subseteq L_x R_x \subseteq W_x$. Inoltre S_x è un aperto di G, poiché intersezione di due aperti. Si ha anche che $1_G \in S_x$ per ogni $x \in C$.

Vale che C è quasi compatto per la topologia indotta da G poiché C è chiuso in G che per ipotesi è quasi compatto. Inoltre $C = \bigcup_{x \in C} (C \cap S_x x)$ poiché se $c \in C$ allora $c \in S_c c$ dato che 1_G appartiene a S_x per ogni x. Poiché $S_x x$ è un aperto di G per ogni $x \in C$ allora $C \cap S_x x$ è un aperto di C per la topologia indotta da G, quindi esistono $n \in \mathbb{N}$ e $x_1, \ldots, x_n \in C$ tali che $C = (C \cap S_{x_1} x_1) \cup \ldots \cup (C \cap S_{x_n} x_n)$. Dunque $C \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i$.

Definiamo ora $S := \bigcap_{i=1}^{n} S_{x_i}$; si ha che S è un aperto di G e che S contiene 1_G. Poiché per ogni i si ha $S \subseteq S_{x_i}$ e poiché abbiamo già visto che $S_x S_x \subseteq W_x$ per ogni x si ha che $S S_{x_i} \subseteq S_{x_i} S_{x_i} \subseteq W_{x_i}$ per ogni i. Dunque

$$SC \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} W_{x_i} x_i \subseteq C$$

allora $SC \subseteq C$ quindi, dato che $1_G \in C$, si ha che $S \subseteq C$.
Sia $T := S \cap S^{-1}$. Vale che T è un aperto di G e che T contiene 1_G. Vale anche che $T = T^{-1}$ infatti se $z \in T$ allora esistono $s, p \in S$ tali che $z = s = p^{-1}$ quindi $p \in S$ e poiché $p = s^{-1}$ si ha anche $p \in S^{-1}$, dunque $p \in T$. Allora $z = p^{-1} \in T^{-1}$. Analogamente si dimostra che che $T^{-1} \subseteq T$.
Definiamo $T^1 := T$; $T^2 := TT^1 = TT$;... ;$T^n := TT^{n-1} = T \cdot \ldots \cdot T$ (n volte). Poiché T è aperto, T^n è aperto per ogni n.
Sia $H := \bigcup_{i=1}^{\infty} T^n$. Si ha che H è un aperto di G. Proviamo che H è un sottogruppo di G. Dato che $1_G \in S$ allora $1_G \in S \cap S^{-1} = T \subseteq H$. Se h_1, $h_2 \in H$ allora esistono $m_1, m_2 \in \mathbb{N}$ tali che $h_1 \in T^{m_1}$, $h_2 \in T^{m_2}$ quindi $h_1 h_2 \in T^{m_1+m_2} \subseteq H$. Se $h \in H$ allora esiste $m \in \mathbb{N}$ tale che $h \in T^m$ dunque esistono $t_1, \ldots, t_m \in T$ tali che $h = t_1 \cdot \ldots \cdot t_m$ quindi $h^{-1} = t_m^{-1} \cdot \ldots \cdot t_1^{-1} \in T^m$, dato che $T^{-1} = T$. Poiché $T^m \subseteq H$ si ha che $h^{-1} \in H$.
Dimostriamo ora per induzione che $T^n \subseteq C$ per ogni $n \in \mathbb{N}$. Dato che $S \subseteq C$ si ha che $T = S \cap S^{-1} \subseteq C$. Supponiamo per ipotesi induttiva che $T^{n-1} \subseteq C$ allora poiché $T \subseteq S$ si ha che $T^n = TT^{n-1} \subseteq SC \subseteq C$. Possiamo quindi affermare che $H = \bigcup_{n=1}^{\infty} T^n \subseteq C$.
Per ipotesi G è quasi compatto e H è un sottogruppo aperto di G allora per l'Osservazione 2.2 punto c) H ha indice finito in G. Esistono quindi $n \in \mathbb{N}$ e $g_1, \ldots, g_n \in G$ tali che $G = g_1 H \cup \ldots \cup g_n H$. Possiamo supporre che per ogni i diverso da j la classe $g_j H$ sia disgiunta dalla classe $g_i H$. Sia $h \in H$ allora esiste g_i tale che $h \in g_i H$ quindi $g_i H = H$. Possiamo dunque assumere che $g_1 \in H$.
Consideriamo il sottogruppo $C_{g_i}(H) := g_i H g_i^{-1}$ di G per ogni i. Proviamo che $\bigcap_{i=1}^{n} C_{g_i}(H)$ è un sottogruppo normale aperto di G contenuto in C terminando così la dimostrazione.

Si ha che $\bigcap_{i=1}^{n} C_{g_i}(H)$ è un sottogruppo di G poiché è intersezione di sottogruppi di G.
Inoltre $\bigcap_{i=1}^{n} C_{g_i}(H)$ è aperto poiché $C_{g_i}(H)$ è aperto per ogni i dato che H è aperto. Poiché $C_{g_1}(H) = g_1 H g_1^{-1} = H$ si ha che $\bigcap_{i=1}^{n} C_{g_i}(H) \subseteq H$.
Per concludere la dimostazione proviamo prima due affermazioni.
La prima affermazione è che dato $i \in \{1, \dots, n\}$ e $g \in G$, se $k \in \{1, \dots, n\}$ è tale che $gg_i \in g_k H$ allora $g\big(\bigcap_{j=1}^{n} C_{g_j}(H)\big)g^{-1} \subseteq C_{g_k}(H)$ per ogni $g \in G$.
Sia $c \in \bigcap_{j=1}^{n} C_{g_j}(H)$ e sia $h \in H$ tale che $gg_i = g_k h$. Si ha che $g_i^{-1} g^{-1} = h^{-1} g_k^{-1}$, ma esiste $h_i \in H$ tale che $c = g_i h_i g_i^{-1}$ quindi

$$gcg^{-1} = gg_i h_i g_i^{-1} g^{-1} = g_k h h_i h^{-1} g_k^{-1},$$

che appartiene a $C_{gk}(H)$ poiché $hh_i h^{-1} \in H$.
La seconda affermazione è che dato $i \in \{1, \dots, n\}$ e $g \in G$, se $k \in \{1, \dots, n\}$ è tale che $gg_i \in g_k H$ allora $gg_j \notin g_k H$ per ogni $j \in \{1, \dots, n\} \setminus \{i\}$.
Infatti per ipotesi esiste $\bar{h} \in H$ tale che $gg_i = g_k \bar{h}$, se per assurdo esiste $h \in H$ tale che $gg_j = g_k h$ allora $(g_k h g_j^{-1}) g_i = gg_i = g_k \bar{h}$ quindi $h g_j^{-1} = \bar{h} g_i^{-1}$ allora $g_j h^{-1} = g_i \bar{h}^{-1}$. Dunque $g_j H \cap g_i H$ è diverso dall'insieme vuoto che è assurdo.
Possiamo ora concludere la dimostrazione.
Sia $g \in G$, esiste $k_1 \in \{1, \dots, n\}$ tale che $gg_1 \in g_{k_1} H$ allora $g\big(\bigcap_{j=1}^{n} C_{g_j}(H)\big)g^{-1} \subseteq C_{g_{k_1}}(H)$ per la prima affermazione.
Per la seconda affermazione per ogni $r \in \{2, \dots, n\}$ l'elemento gg_r non appartiene a $g_{k_m} H$ per ogni $m < r$, allora esiste $k_r \in \{1, \dots, n\} \setminus \{k_1, \dots, k_{r-1}\}$ tale che $gg_r \in g_{k_r} H$ e quindi $g\big(\bigcap_{j=1}^{n} C_{g_j}(H)\big)g^{-1} \subseteq C_{g_{k_r}}(H)$. Risulta dunque dimostrato che per ogni $g \in G$ si ha che $g\big(\bigcap_{j=1}^{n} C_{g_j}(H)\big)g^{-1} \subseteq \bigcap_{j=1}^{n} C_{g_j}(H)$.

□

Proposizione 2.8. *Sia G un gruppo topologico quasi compatto e totalmente disconnesso allora*

a) se U è un aperto di G non vuoto allora U è unione di laterali destri di sottogruppi normali aperti di G.

b) Un insieme P è aperto e chiuso in G se e solo se P è unione finita di laterali destri di sottogruppi normali aperti di G.

c) Sia X un sottoinsieme di G allora

1. $\overline{X} = \bigcap\{NX \text{ con } N \triangleleft_O G\}$.
2. *Per ogni C chiuso di G si ha che* $C = \bigcap\{NC \text{ con } N \triangleleft_O G\}$.
3. $\bigcap\{N \text{ con } N \triangleleft_O G\} = 1_G$.

Dimostrazione. a) Sia U un aperto di G non vuoto. Se $x \in U$ allora Ux^{-1} è un aperto di G contenente 1_G. Poiché per ipotesi G è totalmente disconnesso per il lemma 1.4 punto 3 si ha che Ux^{-1} è unione di insiemi che sono contemporaneamente aperti e chiusi. Fra questi insiemi ne esiste uno, C_x, contenente 1_G. Per il lemma 2.7 poiché C_x è un aperto e chiuso di G contenente 1_G e poiché G è quasi compatto si ha che C_x contiene H_x sottogruppo normale aperto di G. Quindi $Ux^{-1} \supseteq C_x \supseteq H_x$. Dunque per ogni $x \in U$ si ha che $H_x x \subseteq U$ ed essendo H_x un sottogruppo di G, si ha che $1_G \in H_x$ per ogni x. Quindi $U = \bigcup_{x \in U} H_x x$.

b) Sia P è un insieme aperto e chiuso di G. Per il precedente punto di questa dimostrazione poiché P è aperto in G si ha che P è unione di laterali destri di sottogruppi normali aperti di G. Essendo P anche chiuso in G e G quasi comapatto, si ha che P è quasi compatto. Quindi P è unione finita di laterali destri di sottogruppi normali aperti di G.
Viceversa sia $P = \bigcup_{i=1}^{n} H_i x_i$ con H_i sottogruppi normali aperti di G. Allora, poiché $H_i x_i$ per ogni i è aperto, P è aperto. Per l'Osservazione 2.2 punto c), essendo H_i un sottogruppo aperto di G per ogni i, si ha che H_i è anche chiuso in G per ogni i. Allora $H_i x_i$ è chiuso per ogni i e dunque P è anche chiuso.

c) Proviamo prima che $\bigcap\{NX \text{ con } N \triangleleft_O G\} \subseteq \overline{X}$. Sia $y \in NX$ per ogni $N \triangleleft_O G$. Se per assurdo y non appartenesse a $\overline{X}$ allora y apparterrebbe all'insieme aperto $G \setminus \overline{X}$. Esisterebbe allora U_y aperto di G contenente y tale che $U_y \subseteq G \setminus \overline{X} \subseteq G \setminus X$. Si avrebbe inoltre che $U_y y^{-1}$ sarebbe un aperto di G contenente 1_G. Utilizzando argomentazioni analoghe a quelle della dimostrazione a) di questa proposizione si avrebbe che $G \setminus X \supseteq U_y \supseteq Hy$ dove H è un sottogruppo normale e aperto di G. Allora $Hy \cap X = \emptyset$ e quindi y non apparterrebbe ad HX che è assurdo.
Proviamo che $\bigcap\{NX \text{ con } N \triangleleft_O G\} \supseteq \overline{X}$. Se $y \in \overline{X}$ allora per ogni U_y intorno di y in G si ha che $U_y \cap X \neq \emptyset$. Per ogni $N \triangleleft_O G$ si ha che Ny è un intorno di y dunque $Ny \cap X \neq \emptyset$. Quindi per ogni $N \triangleleft_O G$ esistono $n_N \in N$ e $x_N \in X$ tali che $n_N y = x_N$ allora $y \in N x_N \subseteq NX$ per ogni $N \triangleleft_O G$.

Il punto 2 deriva immediatamente dal punto 1.
Il punto 3 si dimostra osservando che poiché G per ipotesi è totalmente disconnesso allora G è anche di Hausdorff per l'Osservazione 2.2 punto f). Sempre per l'Osservazione 2.2 punto f) si ha che 1_G è un chiuso di G, dunque per il punto 2 di questa osservazione si è concluso.

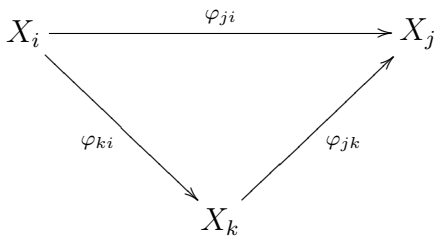
□

Capitolo 3

Sistemi inversi

Definizione 3.1. Sia $(I, \leq)$ un insieme parzialmente ordinato. $(I, \leq)$ è detto insieme diretto se per ogni $i, j \in I$ esiste $k \in I$ tale che $i, j \leq k$.

Definizione 3.2. Un sistema inverso (X_i, φ_{ij}) di spazi topologici indicizzati da un insieme diretto I consiste in una famiglia $(X_i)_{i \in I}$ di spazi topologici e una famiglia $(\varphi_{ij} : X_j \to X_i)_{\substack{i,j \in I \\ i \leq j}}$ di mappe continue con $\varphi_{ii} = id_{X_i}$ per ogni i e tali che $\varphi_{jk} \circ \varphi_{ki} = \varphi_{ji}$ per ogni $i, j, k \in I$ tali che $i \leq k \leq j$, cioè tali che il seguente diagramma, quando è definito, sia commutativo.



Se ogni X_i è un gruppo topologico ed ogni φ_{ij} è un omomorfismo di gruppi continuo si ha un sistema inverso di gruppi topologici. Analogamente si definisce un sistema inverso di anelli.

Esempio 3. *Sia $I = \mathbb{N}$ con la relazione di ordine parziale usuale. Per ogni $i \in \mathbb{N}$ siano X_i degli insiemi finiti, $\varphi_{i,i+1} : X_{i+1} \to X_i$ delle mappe arbitrarie, $\varphi_{ii} = id_{X_i}$ e $\varphi_{ij} = \varphi_{i,i+1} \circ \ldots \circ \varphi_{j-1,j}$ per ogni $j > i$. Si ha che (X_i, φ_{ij}) è un sistema inverso di insiemi finiti.*

Dimostrazione. Ad esempio si ha che la mappa φ_{36} è così costituita
$\varphi_{36} : X_6 \xrightarrow{\varphi_{56}} X_5 \xrightarrow{\varphi_{45}} X_4 \xrightarrow{\varphi_{34}} X_3$, cioè $\varphi_{36} = \varphi_{34} \circ \varphi_{45} \circ \varphi_{56}$.
Dimostriamo che (X_i, φ_{ij}) è un sistema inverso di insiemi finiti.

Chiaramente I è un insieme diretto. Per ogni $j > i$ esiste $s \in \mathbb{N}$ tale che $j = i + s$.
Se $i \leq k \leq i + s$ allora esiste $r \in \mathbb{N}$ tale che $k = i + r$ con $0 \leq r \leq s$, quindi

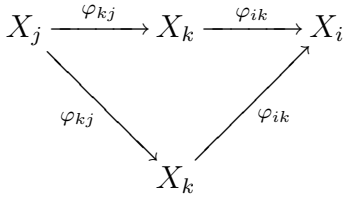
$$\varphi_{ij} = \varphi_{(i+s-1)-(s-1),i+s-(s-1)} \circ \ldots \circ \varphi_{(i+s-1)-(s-r),i+s-(s-r)} \circ \varphi_{(i+s-1)-(s-r-1),i+s-(s-r-1)} \circ \cdots$$

$$\cdots \circ \varphi_{(1+s-1)-1,(i+s)-1} \circ \varphi_{i+s-1,i+s},$$

$$\varphi_{kj} = \varphi_{i+r,i+s} = \varphi_{(i+s-1)-(s-r-1),i+s-(s-r-1)} \circ \ldots \circ \varphi_{i+s-1,i+s},$$

$$\varphi_{ik} = \varphi_{i,i+r} = \varphi_{(i+s-(s-r+1))-(r-1),(i+s-(s-r))-(r-1)} \circ \ldots \circ \varphi_{(i+s-1)-(s-r),i+s-(s-r)}.$$

Quindi il seguente diagramma è commutativo.



□

Esempio 4. *Sia $(S, \leq_S)$ un insieme parzialmente ordinato. Sia I un insieme di sottoinsiemi di S tali che I è un insieme diretto rispetto alla relazione di ordine parziale di inclusione $\subseteq$, cioè $(I, \subseteq)$ è tale che per ogni $i, j \in I$ esiste $k \in I$ tale che $i, j \subseteq k$.*
Sia $X \in I$ (quindi X è un sottoinsieme di S), definiamo

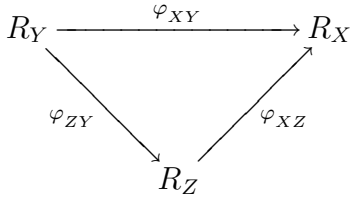
$$R_X := \{\theta : X \to \mathbb{Q} \text{ iniettiva, t.c. per ogni } x_1, x_2 \in X \text{ se } x_1 \leq_S x_2 \text{ allora } \theta(x_1) \leq_{\mathbb{Q}} \theta(x_2)\}$$

Sia $Y \in I$ tale che $Y \supseteq X$, definiamo

$$\begin{array}{rccc} \varphi_{XY} : & R_Y & \longrightarrow & R_X \\ & \theta & \longmapsto & \theta_{|X}. \end{array}$$

Si ha che (R_X, φ_{XY}) è un sistema inverso indicizzato da I.

Dimostrazione. Si noti che $\theta_{|X}$ è ancora iniettiva e conserva ancora l'ordine.
Sia $X \subseteq Z \subseteq Y$, consideriamo il seguente diagramma.



Dobbiamo mostrare che per ogni $\theta \in R_Y$ si ha che $\varphi_{XY}(\theta) = \varphi_{XZ}(\varphi_{ZY}(\theta))$. Per ogni θ si ha $\varphi_{XY}(\theta) = \theta_{|X}$ e $\varphi_{XZ}(\varphi_{ZY}(\theta)) = \varphi_{XZ}(\theta_{|Z}) = (\theta_{|Z})_{|X}$. L'uguaglianza segue osservando che per ogni θ, per ogni $x \in X$ si ha $\theta_{|X}(x) = (\theta_{|Z})_{|X}(x)$.

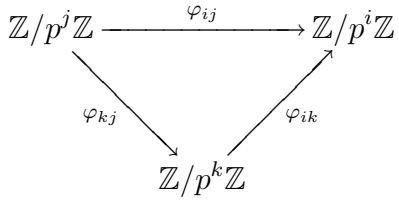
□

Esempio 5. *Siano $I = \mathbb{N}$, p un primo, $G_i := \mathbb{Z}/p^i\mathbb{Z}$ per ogni $i \in \mathbb{N}$. Per ogni $j \geq i$ definiamo*

$$\begin{array}{rccc} \varphi_{ij} : \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ [n]_{p^j} & \longmapsto & [n]_{p^i} \end{array}$$

Si ha che (G_i, φ_{ij}) è un sistema inverso di anelli finiti.

Dimostrazione. Notiamo subito che $\mathbb{Z}/p^j\mathbb{Z}$ è un anello e che le φ_{ij} sono omomorfismi di anelli.
Siano $i \leq k \leq j$, si ha che il seguente diagramma è commutativo.



□

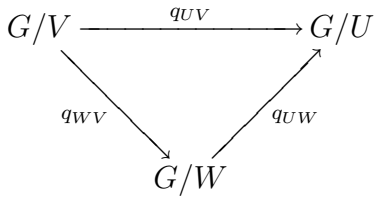
Il seguente esempio ci sarà molto utile durante l'intera tesi.

Esempio 6. *Siano G un gruppo e I una famiglia di sottogruppi normali di G tale che per ogni U_1, $U_2 \in I$ esiste $V \in I$ tale che V è un sottogruppo di $U_1 \cap U_2$ (di seguito chiameremo un insieme con questa proprietà una base filtro). Definiamo in I la relazione $\leq'$ in questo modo: $U \leq' V$ se e solo se V è un sottogruppo di U. Per $U \leq' V$ definiamo*

$$\begin{array}{rccc} q_{UV} : G/V & \longrightarrow & G/U \\ gV & \longmapsto & gU \end{array}$$

Sia ha che $(G/U, q_{UV})$ è un sistema inverso di gruppi.

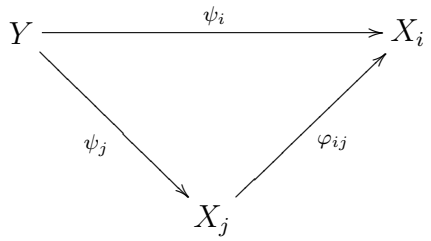
Dimostrazione. Notiamo subito che I è un insieme diretto per $\leq'$ poiché si verifica facilmente che I è una relazione d'ordine e che per ogni U_1, $U_2 \in I$ esiste $V \in I$ tale che U_1, $U_2 \leq' V$ (dato che per ipotesi esiste V sottogruppo di $U_1 \cap U_2$ e quindi V è un sottogruppo sia di U_1 che di U_2).
Si verifica facilmente per $U \leq' V$ che q_{UV} è ben definita ed è un omomorfismo di gruppi.
Verifichiamo che per $U \leq' W \leq' V$ il seguente diagramma è commutativo.



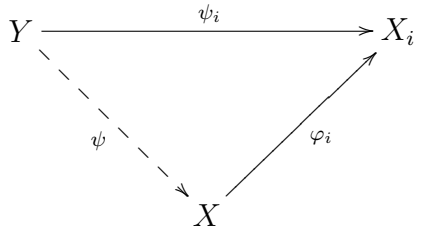
Se $U \leq' W \leq' V$ per ogni $g \in G$ si ha che $q_{UW}(g) \circ q_{WV}(g) = q_{UV}(g)$ se e solo se $gU = q_{UW}(gW)$ che è chiaramente vero.
Si noti che le mappe q_{UV} sono anche suriettive.

□

Definizione 3.3. Sia (X_i, φ_{ij}) un sistema inverso di spazi topologici e sia Y uno spazio topologico. Le mappe continue della famiglia $(\psi_i : Y \to X_i)_{i \in I}$ sono dette compatibili se $\varphi_{ij} \circ \psi_j = \psi_i$ per ogni $i \leq j$ cioè se il seguente diagramma è commutativo:



Definizione 3.4. Un limite inverso (X, φ_i) di un sistema inverso di spazi topologici (rispettivamente gruppi, anelli) è uno spazio topologico (rispettivamente gruppo, anello) X con una famiglia di mappe continue (rispettivamente omomorfismi continui) $(\varphi_i : X \to X_i)$ compatibili con la seguente proprietà universale:
quando $\psi_i : Y \to X_i$ è una famiglia compatibile di mappe continue da uno spazio topologico Y (rispettivamente omomorfismi continui da un gruppo o da un anello) esiste un'unica mappa continua (rispettivamente omomorfismo continuo) $\psi : Y \to X$ tale che $\varphi_i \circ \psi = \psi_i$ per ogni i, cioè esiste ed è unica ψ continua (rispettivamente omomorfismo continuo) tale che il seguente diagramma sia commutativo per ogni i.



Teorema 3.1. *Sia (X_i, φ_{ij}) un sistema inverso indicizzato da I.*

1. *se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ sono limiti inversi del sistema inverso (X_i, φ_{ij}) allora esiste un'unico isomorfismo $\bar{\varphi} : X^{(1)} \to X^{(2)}$ tale che $\varphi_i^{(2)} \circ \bar{\varphi} = \varphi_i^{(1)}$ per ogni i ($\bar{\varphi}$ è un omeomorfismo se le X_i sono spazi topologici).*

2. *Siano*

$$\begin{array}{rccc} p_j : \prod_{i \in I} X_i & \longrightarrow & X_j \\ (x_i)_{i \in I} & \longmapsto & x_j, \end{array}$$

$$X := \{x \in \prod_{i\in I} X_i \text{ tali che } \varphi_{ij} \circ p_j(x) = p_i(x) \text{ per ogni } i, j \text{ con } j \geq i\},$$

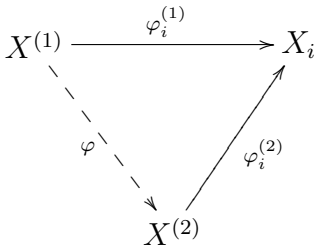
e

$$\varphi_i := p_{i|X}.$$

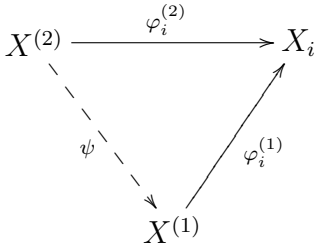
Allora (X, φ_i) *è un limite inverso di* (X_i, φ_{ij}).

3. *Se* (X_i, φ_{ij}) *è un sistema inverso di gruppi topologici e omomorfismi continui allora* X *è un gruppo topologico e le* φ_i *sono omomorfismi continui.*

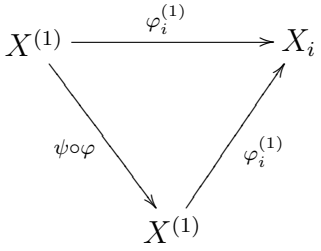
Dimostrazione. 1. Poiché $X^{(2)}$ è un limite inverso e $(\varphi_i{}^{(1)})_{i\in I}$ sono una famiglia di mappe continue compatibili con (X_i, φ_{ij}), esiste ed è unica φ continua tale che $\varphi_i^{(2)} \circ \varphi = \varphi_i^{(1)}$ per ogni i.



Dimostriamo che φ è un omeomorfismo.
Analogamente $X^{(1)}$ è un limite inverso e $(\varphi_i^{(2)})_{i\in I}$ sono una famiglia di mappe continue compatibili con (X_i, φ_{ij}) e quindi esiste ψ continua tale che $\varphi_i^{(1)} \circ \psi = \varphi_i^{(2)}$ per ogni i.

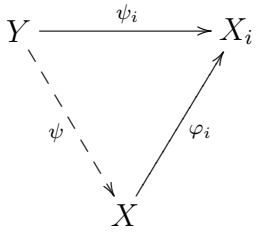


Abbiamo dunque che $(\varphi_i^{(1)} \circ \psi) \circ \varphi = \varphi_i^{(1)} \circ (\psi \circ \varphi) = \varphi_i^{(1)}$ per ogni i e $(\varphi_i^{(2)} \circ \varphi) \circ \psi = = \varphi_i^{(2)} \circ (\varphi \circ \psi) = \varphi_i^{(2)}$ per ogni i.



Ma anche $id_{X^{(1)}}$ è tale che $\varphi_i^{(1)} \circ id_{X^{(1)}} = \varphi_i^{(1)}$ per ogni i e quindi, essendo le $\varphi_i^{(1)}$ compatibili, per la proprietà universale di $X^{(1)}$ si ha che $\psi \circ \varphi = id_{X^{(1)}}$.
Analogamente $id_{X^{(2)}}$ è tale che $\varphi_i^{(2)} \circ id_{X^{(2)}} = \varphi_i^{(2)}$ per ogni i e per la proprietà universale di $X^{(2)}$ abbiamo che $\varphi \circ \psi = id_{X^{(2)}}$.
Quindi φ è continua, biunivoca e con inversa continua.

2. Poiché consideriamo $\prod_{i \in I} X_i$ con la topologia prodotto e X con la topologia indotta si ha che le φ_i sono continue. Le φ_i sono compatibili se e solo se per ogni $x \in X$ si ha che $\varphi_{ij} \circ \varphi_j(x) = \varphi_i(x)$ per ogni $j \geq i$, che risulta essere vero per definizione di X.
Sia $(\psi_i : Y \to X_i)_{i \in I}$ una famiglia di mappe continue compatibili, vogliamo dimostrare che esiste ed è unica ψ continua tale che $\varphi_i \circ \psi = \psi_i$ per ogni i.



Dimostriamo l'esistenza, consideriamo la seguente mappa.

$$\begin{aligned} \psi : Y &\longrightarrow \prod_{i \in I} X_i \\ y &\longmapsto (\psi_i(y))_{i \in I} \end{aligned}$$

La mappa ψ è continua poiché $p_i \circ \psi = \psi_i$ è continua per ogni i.
Dimostriamo ora che per ogni $y \in Y$ si ha $\psi(y) \in X$. Per ogni $y \in Y$ dimostrare che $\psi(y) \in X$ vuol dire verificare che per ogni $y \in Y$, per ogni $j \geq i$ si ha che $\varphi_{ij} \circ p_j(\psi(y)) = p_i(\psi(y))$ che risulta essere vero poiché per ipotesi le ψ_j sono compatibili quindi per ogni $y \in Y$, per ogni $j \geq i$ si ha che $\varphi_{ij} \circ \psi_j(y) = \psi_i(y)$. Se restringiamo il codominio della mappa ψ abbiamo dimostrato l'esistenza.
Dimostriamo ora l'unicità. Sia $\psi' : Y \to X$ continua tale che $\varphi_i \circ \psi' = \psi_i$ per ogni i allora per ogni $y \in Y$ si ha che $p_{i|X}(\psi'(y)) = \psi_i(y) = p_{i|X}(\psi(y))$ per ogni i quindi $\psi' = \psi$.

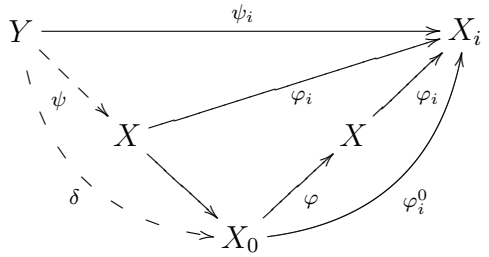
3. Poiché le X_i sono gruppi topologici allora $\prod X_i$ è un gruppo topologico (Osservazione 2.1 punto 3). Si può verificare facilmente che X è un sottogruppo di $\prod X_i$ poiche le φ_{ij} sono omomorfismi di gruppi, e quindi per l'Osservazione 2.1 punto 2 X è un gruppo topologico con la topologia indotta.

□

Poiché un limite inverso di un sistema inverso (X_i, φ_{ij}) è univocamente determinato a meno di isomorfismi spesso si dice 'il' limite inverso di un sistema inverso. Tale limite verrà indicato con $\varprojlim (X_i, \varphi_{ij})$ oppure con $\varprojlim X_i$. Il limite inverso costruito nella dimostrazione precedente è denotato con $s\varprojlim X_i$.

Osservazione 3.2. *Sia (X_i, φ_{ij}) un sistema inverso di spazi topologici e sia (X, φ_i) un suo limite inverso. Siano X_0 uno spazio topologico e $\varphi : X_0 \longrightarrow X$ un omemorfismo. Allora (X_0, φ_i^0) è un limite inverso di (X_i, φ_{ij}), con $\varphi_i^0 := \varphi_i \circ \varphi$.*

Dimostrazione. Dimostriamo prima che le φ_i^0 sono compatibili ovvero che per ogni $i \leq j$ si ha che $\varphi_{ij} \circ \varphi_j^0 = \varphi_i^0$, che risulta essere vero poiché le φ_i sono compatibili e per come sono definite le φ_i^0. Dimostriamo ora che la proprietà universale del limite inverso vale per (X_0, φ_i^0). Siano $\psi_i : Y \longrightarrow X_i$ compatibili allora esiste ed è unica $\psi : Y \longrightarrow X$ continua tale che $\varphi_i \circ \psi = \psi_i$ per ogni i.



Chiaramente per $\delta = \varphi^{-1} \circ \psi$ si ha $\varphi_i^0 \circ \delta = \psi_i$ per ogni i. Se inoltre δ è un altra applicazione tale che $\varphi_i^0 \circ \delta = \psi_i$ per ogni i allora $\varphi_i \circ (\varphi \circ \delta) = \psi_i = \varphi_i \circ \psi$ per ogni i, dunque per l'unicità della ψ si ha che $\varphi \circ \delta = \psi$, allora $\delta = \varphi^{-1} \circ \psi$.

□

Proposizione 3.3. *Sia $(X_i, \varphi_{ij})_{i \in I}$ un sistema inverso di spazi topologici indicizzato da I, poniamo $X := \varprojlim X_i$.*

1. *Se X_i è uno spazio topologico di Hausdorff per ogni i allora X è di Hausdorff.*
2. *Se X_i è uno spazio topologico totalmente disconnesso per ogni i allora X è totalmente disconnesso.*
3. *Se X_i è uno spazio topologico di Hausdorff per ogni i allora $s\varprojlim X_i$ è chiuso in $(\prod_{i \in I} X_i, \mathcal{P})$.*
4. *Se X_i è uno spazio topologico quasi compatto e di Hausdorff per ogni i allora X è quasi compatto e di Haudorff.*

5. *Se X_i è uno spazio topologico diverso dall'insieme vuoto, di Haudorff, quasi compatto per ogni i allora X è diverso dall'insieme vuoto.*

Dimostrazione. 1. Proviamo che $s\varprojlim X_i$ è di Hausdorff, se ciò vale anche tutti gli altri limiti inversi sono di Hausdorff poiché omeomorfi a $s\varprojlim X_i$.

Si ha che $s\varprojlim X_i$ è un sottoinsieme di $\prod_i X_i$ munito della topologia indotta. Poiché X_i è di Hausdorff allora $(\prod X_i, \mathcal{P})$ è di Hausdorff, quindi $s\varprojlim X_i$ è di Hausdorff.

2. Proviamo che $s\varprojlim X_i$ è totalmente disconnesso, se ciò vale la dimostrazione è conclusa per l'Osservazione 1.3. Dato che gli X_i sono totalmente disconnessi per ogni i per l'Osservazione 1.2 si ha che $\prod X_i$ è totalmente disconnesso, ma $s\varprojlim X_i$ è un sottospazio topologico di $\prod X_i$, allora per l'Osservazione 1.1 $s\varprojlim X_i$ è totalmente disconnesso.

3. Si usa il seguente noto fatto: se $f, g : X \longrightarrow Y$ sono applicazioni continue e Y è di Hausdorff allora l'insieme

$$\{x \in X \text{ tali che } f(x) = g(x)\}$$

è un chiuso in X.

$$s\varprojlim X_i = \{x \in \prod_{i\in I} X_i \text{ tale che } \varphi_{ij} \circ p_j(x) = p_i(x) \text{ per ogni } i, j \text{ con } j \geq i\} =$$

$$= \bigcap_{j\geq i} \{x \in \prod_{i\in I} X_i \text{ tale che } \varphi_{ij} \circ p_j(x) = p_i(x)\}.$$

Poiché le mappe p_i sono continue per ogni i e le mappe φ_{ij} sono continue per ogni $j \geq i$ si ha che $\{x \in \prod_i X_i \text{ tale che } \varphi_{ij} \circ p_j(x) = p_i(x)\}$ è un chiuso di $\prod X_i$. Quindi $s\varprojlim X_i$ è intersezione di chiusi di $\prod X_i$ dunque è un chiuso di $\prod X_i$.

4. Per il primo punto di questa proposizione sappiamo già che $\varprojlim X_i$ è di Hausdorff. Se dimostriamo che $s\varprojlim X_i$ è quasi compatto allora ogni altro limite inverso è quasi compatto poiché la quasi compattezza si conserva per continuità. Poiché le X_i sono quasi compatte per ogni i allora per il teoreama di Tychonoff $\prod X_i$ è quasi compatto[1]. Per il punto 3 di questa proposizione si ha che $s\varprojlim X_i$ è un chiuso di $\prod X_i$ quindi anche $s\varprojlim X_i$ è quasi compatto.

[1]Per una dimostrazione del teorema di Tychonoff si veda ad esempio il libro *Profinite Groups* di J.S. Wilson [8].

5. Per ogni $j \geq i$ con $i, j \in I$ sia $D_{ij} := \{x \in \prod_i X_i \text{ tale che } \varphi_{ij} \circ p_j(x) = p_i(x)\}$. D_{ij} è chiuso in $\prod_i X_i$ per ogni $j \geq i$ poiché $\varphi_{ij} \circ p_j$ e le $p_i(x)$ sono continue e gli spazi X_i sono di Hausdorff per ogni i come nel punto 3 della dimostrazione. Essendo gli X_i quasi compatti, per il teorema di Tychonoff lo spazio $(\prod_i X_i, \mathcal{P})$ è quasi compatto. Se per assurdo $s\varprojlim X_i = \emptyset$ allora $(D_{ij})_{j \geq i}$ costituisce una famiglia di chiusi di $\prod_i X_i$ la cui intersezione è l'insieme vuoto e dunque per la quasi compattezza di $\prod_i X_i$ esistono $(i_i, j_1), \ldots, (i_n, j_n)$ con $j_r \geq i_r$ tali che $\bigcap_{r=1}^{n} D_{i_r j_r} = \emptyset$. Poiché I è un insieme diretto esiste $k \in I$ tale che $k \geq j_r$ per ogni $r = 1, \ldots, n$. Sia $x_k \in X_k \neq \emptyset$ e sia $x_l := \varphi_{lk}(x_k)$ per ogni l con $l \leq k$. Costruiamo un elemento che appartiene a $\bigcap_{r=1}^{n} D_{i_r j_r}$ ottenendo così l'assurdo. Definiamo $\tilde{x} := (x_l)_{l \in I} \in \prod_i X_i$ dove x_l è arbitrario per ogni $l > k$.
Proviamo che $\varphi_{i_r j_r} \circ p_{j_r}((x_l)_{l \in I}) = p_{i_r}((x_l)_{l \in I})$ per ogni $r = 1, \ldots, n$. Si ha che $\varphi_{i_r j_r} \circ p_{j_r}((x_l)_{l \in I}) = p_{i_r}((x_l)_{l \in I})$ se e solo se $\varphi_{i_r j_r}(x_{j_r}) = x_{i_r}$. Siccome $i_r \leq j_r \leq k$ per ogni r allora $x_{i_r} = \varphi_{i_r k}(x_k)$ e $x_{j_r} = \varphi_{j_r, k}(x_k)$. Poiché $\varphi_{i_r j_r} \circ \varphi_{j_r k}(x_k) = \varphi_{i_r k}(x_k)$ per ogni r dato che (X_i, φ_{ij}) è un sistema inverso si ha allora $\varphi_{i_r j_r}(x_{j_r}) = x_{i_r}$ per ogni r e così si ha ciò che volevamo provare.
Si è ottenuto dunque che $(x_l)_{l \in I} \in \bigcap_{r=1}^{n} D_{i_r, j_r} = s\varprojlim X_i$, che è assurdo.
Ogni altro limite inverso deve essere diverso dall'insieme vuoto poiché è isomorfo a $s\varprojlim X_i$.

□

Proposizione 3.4. *Sia (X, φ_i) un limite inverso di un sistema inverso (X_i, φ_{ij}) indicizzato da I, dove gli X_i sono spazi topologici diversi dall'insieme vuoto, quasi compatti e di Hausdorff.*
Allora

1. $\varphi_i(X) = \bigcap_{j \geq i} \varphi_{ij}(X_j)$ *per ogni* $i \in I$.

2. *Gli insiemi* $\varphi_i^{-1}(U)$ *con* $i \in I$ *e* U *aperto di* X_i *formano una base per la topologia di* X.

3. *Se* Y *è un sottoinsieme di* X *tale che* $\varphi_i(Y) = X_i$ *per ogni* $i \in I$ *allora* Y *è denso in* X.

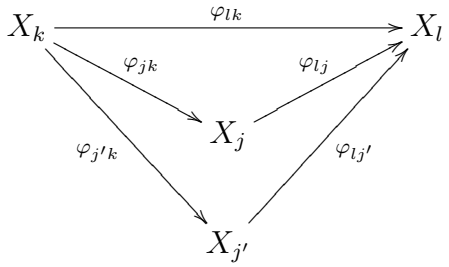
4. Una mappa $\theta : Y \longrightarrow X$ è continua se e solo se $\varphi_i \circ \theta$ è continua per ogni $i \in I$.

Dimostrazione. 1. Dimostriamo prima che se la tesi vale per $X = s\varprojlim X_i$ allora vale anche per ogni altro limite inverso. Supponiamo quindi che $p_{i_{|(s\varprojlim X_i)}}(s\varprojlim X_i) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni i e sia $(X^{(2)}, \varphi_i^{(2)})$ un altro limite inverso. Sappiamo per il Teorema 3.1 che esiste $\bar{\varphi} : s\varprojlim X_i \longrightarrow X^{(2)}$ tale che $\varphi_i^{(2)} \circ \bar{\varphi} = \varphi_i = p_{i_{|(s\varprojlim X_i)}}$. Poiché $p_{i_{|(s\varprojlim X_i)}}(s\varprojlim X_i) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni i allora $\varphi_i^{(2)}(\bar{\varphi}(s\varprojlim X_i)) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogn i e dunque $\varphi_i^{(2)}(X^{(2)}) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni i, da cui segue quanto voluto.
Per facilità di notazione poniamo $X := s\varprojlim X_i$ e $\varphi_i := p_{i_{|(s\varprojlim X_i)}}$, dimostriamo dunque che $\varphi_i(X) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni $i \in I$.
Dimostriamo prima che $\varphi_i(X) \subseteq \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni $i \in I$.
Sia $i \in I$, poiché le φ_i sono compatibili per ogni $j \geq i$ si ha che $\varphi_i = \varphi_{ij} \circ \varphi_j$, allora $\varphi_i(X) = \varphi_{ij} \circ \varphi_j(X) \subseteq \varphi_{ij}(X_j)$ per ogni $j \geq i$ e quindi $\varphi_i(X) \subseteq \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni $i \in I$.
Dimostriamo ora che $\varphi_i(X) \supseteq \bigcap_{j\geq i} \varphi_{ij}(X_j)$ per ogni $i \in I$.
Fissiamo i. Se $\bigcap_{j\geq i} \varphi_{ij}(X_j)$ è uguale all'insieme vuoto abbiamo finito. In caso contrario sia $a \in \bigcap_{j\geq i} \varphi_{ij}(X_j) \subseteq X_i$ vogliamo dimostrare che $a \in \varphi_i(X)$ cioè che esiste $b \in X$ tale che $\varphi_i(b) = a$. Vogliamo costruire tale $b = (b_l)_{l\in I}$. Per $j \geq i$ sia

$$Y_j := \{y \in X_j \text{ tale che } \varphi_{ij}(y) = a\} = \varphi_{ij}^{-1}(a)$$

con la topologia indotta dagli spazi X_j. Per ogni $j \geq i$, poiché $a \in \varphi_{ij}(X_j)$, gli spazi Y_j sono non vuoti. Poichè gli spazi X_i sono di Hausdorff ogni loro punto è un chiuso di X_i. Quindi poiché le mappe φ_{ij} sono continue gli spazi Y_j sono chiusi. Dal fatto che gli spazi Y_j sono chiusi e dal fatto che gli spazi X_j sono quasi compatti e di Haudorff segue che gli Y_j sono quasi compatti e di Hausdorff. Notiamo ora che $(Y_j, \varphi_{rj_{|Y_j}} : Y_j \longrightarrow Y_r)_{r,\underset{j\geq r}{j\geq i}}$ è ancora un sistema inverso.
L'insieme $\{j \geq i \text{ tale che } i \in I\}$ è chiaramente ancora un insieme diretto. Notiamo che $\varphi_{rj_{|Y_j}}(Y_j) \subseteq Y_r$ per $j \geq r$. Dobbiamo mostrare che per $j \geq r$, per ogni $y_j \in Y_j$

si ha che $\varphi_{rj}(y_j) \in Y_r$, che equivale a dimostrare che per $j \geq r$, per ogni $y_j \in Y_j$ si ha che $\varphi_{ir}(\varphi_{rj}(y_j)) = a$. Poiché $y_j \in Y_j$ si ha che $\varphi_{ij}(y_j) = a$, inoltre poiché le mappe φ_{ij} fanno parte di un sistema inverso per ogni $j \geq r$ si ha che $\varphi_{ir} \circ \varphi_{rj} = \varphi_{ij}$. Quindi risulta verificato che $\varphi_{rj_{|Y_j}}(Y_j) \subseteq Y_r$ per $j \geq r$.
Le $\varphi_{rj_{|Y_j}}$ sono ancora continue e per ogni $j \geq s \geq r$ si ha che $\varphi_{rj_{|Y_j}} = \varphi_{rs_{|Y_s}} \circ \varphi_{sj_{|Y_j}}$ poiché ciò vale per le φ_{ij}.
Possiamo dunque concludere che poiché gli spazi Y_j sono non vuoti e sono compatti allora $s\varprojlim_{j \geq i} Y_j$ è non vuoto. Sia $(b_j)_{j \geq i} \in s\varprojlim_{j \geq i} Y_j$. Per definizione di $s\varprojlim_{j \geq i} Y_j$ si ha che $\varphi_{rj}(b_j) = b_r$ per ogni $j \geq r \geq i$ e $\varphi_{ir}(b_r) = b_i$, allora $b_i = a$.
Vogliamo ora completare $(b_j)_{j \geq i}$ a $(b_l)_{l \in I}$.
Sia $l \in I$ con $l < i$ allora poiché I è diretto esiste $j \in I$ tale che $j \geq i, l$. Sia $b_l := \varphi_{lj}(b_j)$ per ogni $l < i$. La definizione di b_l per $l < i$ è indipendente dalla j scelta, sia infatti $j' \geq i, l$ dimostriamo che $b_l := \varphi_{lj}(b_j) = \varphi_{lj'}(b_{j'})$. Poiché I è diretto esiste $k \in I$ tale che $k \geq j, j'$. Poiché $k \geq j \geq i$ si ha che $b_j = \varphi_{jk}(b_k)$ e poiché $k \geq j' \geq i$ si ha che $b_{j'} = \varphi_{j'k}(b_k)$, dunque $\varphi_{lj}(b_j) = \varphi_{lj}(\varphi_{jk}(b_k)) = \varphi_{lk}(b_k) = = \varphi_{lj'} \circ \varphi_{j'k}(b_k) = \varphi_{lj'}(b_{j'})$.



Riassumiamo, per $l < i$ si ha $b_l := \varphi_{lj}(b_j)$ con $j \geq l > i$ indipendente dalla scelta di j, per $l \geq i$ si ha $b_l = p_l((b_r)_{r \geq i})$ con $(b_r)_{r \geq i} \in s\varprojlim_{j \geq i} Y_j$.
Per ogni $l \in I$ per ogni $k \geq l$ si ha $b_l = \varphi_{lk}(b_k)$: se $l < i$ è vero per definizione, se $l \geq i$ poiché $b_l = p_l((b_r)_r) = \varphi_{lk}(p_k((b_r)_r)) = \varphi_{lk}(b_k)$.
Poiché

$$s\varprojlim_{i \in I} Y_i = \{y \in \prod_{i \in I} Y_i \text{ tale che } \varphi_{ij} \circ p_j(y) = p_i(y) \text{ per ogni } i, j \text{ con } j \geq i\}$$

allora $(b_l)_{l \in I} \in s\varprojlim_{i \in I} Y_i$. Ma $s\varprojlim_{i \in I} Y_i \subseteq s\varprojlim X_i = X$ e vale $\varphi_i((b_l)_l) = = p_{i_{|s\varprojlim X_i}}((b_l)_l) = b_i = a$ allora esiste $b \in X$ tale che $\varphi_i(b) = a$.

2. Se dimostriamo che l'affermazione vale per $s\varprojlim X_i$ allora vale per ogni altro limite inverso. Sia infatti $(X^{(1)}, \varphi_i^{(1)})$ un altro limite inverso, vorremmo che la famiglia $(\varphi_i^{(1)})^{-1}(U)$ con $i \in I$, U aperto di X_i formasse una base per $X^{(1)}$. Per il Teorema

3.1 esiste un omeomorfismo $\bar{\varphi} : X^{(1)} \longrightarrow s\varprojlim X_i$ tale che, posto $\varphi_i := p_{i|(s\varprojlim X_i)}$, si ha $\varphi_i^{(1)} = \varphi_i \circ \bar{\varphi}$. Si ha dunque che $(\varphi_i^{(1)})^{-1}(U) = (\varphi_i \circ \bar{\varphi})^{-1}(U) = \bar{\varphi}^{-1} \circ (\varphi_i)^{-1}(U)$ che formano una base per $X^{(1)}$ al variare di i e di U poiché gli insiemi $(\varphi_i)^{-1}(U)$ formano una base per $s\varprojlim X_i$ e poiché $\bar{\varphi}^{-1}$ è un omeomorfismo.
Per facilità di notazione poniamo $X := s\varprojlim X_i$ e $\varphi_i := p_{i|(s\varprojlim X_i)}$.

Sappiamo che una base per $\prod_i X_i$ con la topologia prodotto è

$$\mathcal{B} = \{B = \prod A_i, \text{ con } A_i \in \tau_i, A_i = X_i \text{ eccetto che per un numero finito di } i\}.$$

Se $B \in \mathcal{B}$ esistono $n \in \mathbb{N}$, $A_{i_s} \in \tau_{i_s}$ tali che $B = p_{i_1}^{-1}(A_{i_1}) \cap \ldots \cap p_{i_n}^{-1}(A_{i_n})$ e quindi

$$\mathcal{B} = \{B = p_{i_1}^{-1}(A_{i_1}) \cap \ldots \cap p_{i_n}^{-1}(A_{i_n}) \text{ con } n \in \mathbb{N}, A_{i_r} \in \tau_{i_r} \text{per ogni } r = 1 \ldots n\}.$$

Un aperto di X è dunque dato dall'unione di insiemi del tipo $P := X \cap B$ con $B \in \mathcal{B}$.
Fissiamo

$$P = X \cap p_{i_1}^{-1}(A_{i_1}) \cap \ldots \cap p_{i_n}^{-1}(A_{i_n}),$$

dimostriamo che per ogni $a \in P$ esistono $k \in I$ dipendente da a, U aperto di X_k dipendente da a, tale che $a \in \varphi_k^{-1}(U)$ e tale che $\varphi_k^{-1}(U) \subseteq P$. Se ciò vale l'unione al variare di a di tutti gli insiemi $\varphi_k^{-1}(U)$ è uguale a P. Di conseguenza qualsiasi aperto di X essendo unione di aperti della forma di P sarà unione di aperti del tipo $\varphi_k^{-1}(U)$.
Sia $a = (a_i)_{i \in I} \in P$. Costruiamo un aperto U di X_k tale che $a \in \varphi_k^{-1}(U) \subseteq P$, con k opportuno.
Poiché I è un insieme diretto esiste $k \in I$ tale che $k \geq i_1, \ldots, i_n$. Chiaramente $\varphi_{i_r k}^{-1}(A_{i_r})$ è aperto in X_k per ogni $r = 1, \ldots, n$ essendo $\varphi_{i_r k}$ continua per ogni r.
Mostriamo che $a_k \in \varphi_{i_r k}^{-1}(A_{i_r})$ per ogni r. Per ogni r si ha che $\varphi_{i_r k}(a_k) = = \varphi_{i_r k}(p_k((a_i)_{i \in I}) = p_{i_r}((a_i)_{i \in I}) = a_{ir}$, dato che $a \in X$. Inoltre $a \in p_{i_r}^{-1}(A_{i_r})$ per ogni r allora $a_{i_r} \in A_{i_r}$ per ogni r. Quindi $\varphi_{i_r k}(a_k) \in A_{i_r}$ per ogni r.
Sia $U := \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(A_{i_r})$. Si ha che U è un aperto di X_k poiché intersezione di aperti e $a_k \in U$. Allora $\varphi_k^{-1}(U)$ è un aperto di X e $a \in \varphi_k^{-1}(U)$ (poiché $\varphi_k(a) = p_{k|X}(a) = = a_k$).
Se dimostriamo che $\varphi_k^{-1}(U) \subseteq P$ la dimostrazione è conclusa. Vogliamo dimostrare che se $b = (b_i)_{i \in I} \in \varphi_k^{-1}(U) \subseteq X$, allora $b \in p_{i_r}^{-1}(A_{i_r})$ per ogni $r = 1, \ldots, n$ cioè che $b_{i_r} \in A_{i_r}$ per ogni r.
Se $b = (b_i)_{i \in I} \in \varphi_k^{-1}(U)$ allora $\varphi_k(b) = b_k \in U$, quindi $\varphi_{i_r k}(b_k) \in A_{i_r k}$ per ogni r. Poiché $b \in X$ e $k \geq i_r$ per ogni $r = 1, \ldots, n$, si ha che $\varphi_{i_r k}(b_k) = b_{i_r}$ per ogni r allora $b_{i_r} \in A_{i_r k}$ per ogni r.

3. Dimostriamo che ogni punto $x \in X$ è aderente a Y, cioè che per ogni intorno U_x di x, si ha che $U_x \cap Y$ è diverso dall'insieme vuoto. Basta dimostrare che per ogni aperto A di X, l'insieme $A \cap Y$ è non vuoto, che vale anche se lo si dimostra solo per gli elementi di una base per la topologia di X. Per il precedente punto della dimostrazione sappiamo come è fatta una base per la topologia di X e quindi dobbiamo solo dimostrare che per ogni $i \in I$ per ogni U^i aperto di X_i, l'insieme $\varphi^{-1}(U^i) \cap Y$ è diverso dal vuoto.
   Per ogni $i \in I$ e per ogni U^i aperto di X_i si ha che l'insieme $\varphi_i(Y) \cap U^i$ è non vuoto poiché per ipotesi $\varphi_i(Y) = X_i$. Esistono quindi $y \in Y$ e $u^i \in U^i$ tali che $\varphi_i(y) = u^i$, allora $y \in \varphi_i^{-1}(U^i) \cap Y$, che dimostra quanto voluto.

4. Se θ è continua allora $\varphi_i \circ \theta$ è continua per ogni i poiché le φ_i sono continue per ogni i.
   Dimostriamo che θ è continua nel caso che $\varphi_i \circ \theta$ sia continua per ogni i. La mappa θ è continua se e solo se per ogni B aperto di X si ha che $\theta^{-1}(B)$ è un aperto di Y. Per il punto 2 di questa proposizione esiste J sottoinsieme di I, esistono U^j aperti di X_j per ogni $j \in J$ tali che $B = \bigcup_{j \in J} \varphi_j^{-1}(U^j)$ allora $\theta^{-1}(B) = \bigcup_{j \in J} \theta^{-1}(\varphi_j^{-1}(U^j)) =$
   $= \bigcup_{j \in J} (\varphi_j \circ \theta)^{-1}(U^j)$ che è un aperto di Y poiché $\varphi_j \circ \theta$ sono continue per ogni j.

□

Proposizione 3.5. *Sia X uno spazio topologico quasi compatto, di Hausdorff e totalmente disconnesso. Allora X è il limite inverso dei suoi spazi quoziente discreti.*

Dimostrazione. Sia I l'insieme di tutte le partizioni di X in un numero finito di insiemi aperti e chiusi. I è chiaramente diverso dall'insieme vuoto, ad esempio $\{X, \emptyset\} \in I$.
Per ogni $i \in I$, $i = \{A_1^i, \ldots, A_{n_i}^i\}$ definiamo la relazione di equivalenza $\sim_i$ in questo modo: sia $x \in X$ allora esiste ed e è unico A_j tale che $x \in A_j$, per ogni $y \in X$ diciamo che $y \sim_i x$ se e solo se $y \in A_j$. Definiamo lo spazio topologico $X_i := X/\sim_i$ con la topologia quoziente. Lo spazio X_i è finito poiché i suoi elementi sono gli aperti e chiusi che formano la partizione.
Definiamo per ogni $i \in I$ le mappe continue q_i così:

$$\begin{array}{rccc} q_i : X & \longrightarrow & X_i \\ x & \longmapsto & [x]_{\sim_i}. \end{array}$$

X_i con la topologia quoziente è discreto, infatti ogni elemento di X_i è un aperto per $\mathcal{Q}$ poiché $q_i^{-1}([x]_{\sim_i}) = A_r^i$ è aperto in X. Quindi ogni X_i è uno spazio quoziente discreto.
Viceversa se $(X/\!\sim, \mathcal{Q})$ è un altro spazio quoziente di X discreto allora $X/\!\sim$ è finito ed esiste $i \in I$ tale che $X/\!\sim = X/\!\sim_i$. Infatti $\pi(X) = X/\!\sim$, dove π è la mappa quoziente. Allora, essendo X quasi compatto, $X/\!\sim$ è quasi compatto dunque esistono $[x_1]_\sim, \ldots, [x_n]_\sim \in X/\!\sim$

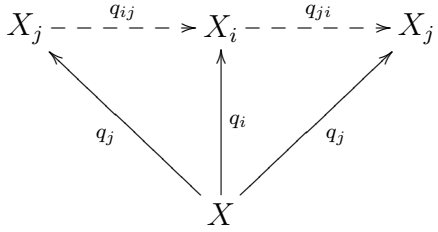
tali che

$$X/\!\sim = \bigcup_{x\in X} [x]_\sim = [x_1]_\sim \cup \ldots \cup [x_n]_\sim$$

e quindi $X/\!\sim$ è un insieme finito. Possiamo supporre gli elementi $[x_1]_\sim, \ldots, [x_n]_\sim$ distinti. Inoltre

$$X = \pi^{-1}(X/\!\sim) = \pi^{-1}([x_1]_\sim) \cup \ldots \cup \pi^{-1}([x_n]_\sim)$$

da cui facilmente deriva che $i_0 := \{\pi^{-1}([x_1]_\sim), \ldots, \pi^{-1}([x_n]_\sim)\}$ è una partizione di X costituita da insiemi sia aperti che chiusi di X. Si può inoltre facilmente verificare che la relazione $\sim$ coincide con la relazione $\sim_{i_0}$.
Siano $i, j \in I$ definiamo la relazione $\leq$ fra elementi di I in questo modo: $i \leq j$ se e solo se esiste una mappa continua $q_{ij} : X_j \longrightarrow X_i$ tale che $q_i = q_{ij} \circ q_j$. La mappa q_{ij} è univocamente determinata poiché se $q'_{ij} : X_j \longrightarrow X_i$ è un'altra mappa continua con la stessa proprietà allora $q_{ij}(q_j(x)) = q'_{ij}(q_j(x))$ per ogni $x \in X$ e quindi $q_{ij} = q'_{ij}$ essendo q_j suriettiva.
Dimostriamo che I con la relazione $\leq$ risulta un insieme parzialmente ordinato. Per ogni $i \in I$ si ha che $i \leq i$, poiché basta considerare $q_{ii} = id_{X_i}$. Se $i \leq j$ e $j \leq k$ allora $i \leq k$, poiché basta considerare la composizione delle mappe. Rimane da dimostrare che se $i \leq j$ e $j \leq i$ allora $i = j$, intendendo l'uguaglianza fra insiemi. Si ha che esistono q_{ij}, q_{ji} mappe continue tali che $q_i = q_{ij} \circ q_j$ e $q_j = q_{ji} \circ q_i$ allora $q_i = q_{ij} \circ q_{ji} \circ q_i$ e $q_j = q_{ji} \circ q_{ij} \circ q_j$ quindi essendo q_i e q_j suriettive $q_{ij} \circ q_{ji} = id_{x_j}$ e $q_{ji} \circ q_{ij} = id_{X_j}$ dunque q_{ij} è un omeomorfismo fra X_j e X_i ed in particolare una applicazione biunivoca.



Gli spazi X_j e X_i hanno così lo stesso numero di elementi e quindi le partizioni i e j hanno lo stesso numero di elementi.
Inoltre sia $i = \{U_1, \ldots, U_m\}$ e $j = \{V_1, \ldots, V_m\}$. Se $y_0 \in U_1$ allora esiste r tale che $y_0 \in V_r$. Se y è un altro elemento di U_1 allora $q_{ji}(q_i(y)) = q_{ji}([y]_{\sim_i}) = q_j(y) = [y]_{\sim_j}$, ma, poiché $[y]_{\sim_i} = [y_0]_{\sim_i}$ si ha che $[y]_{\sim_j} = [y_0]_{\sim_j}$ e quindi anche $y \in V_r$ dunque $U_1 \subseteq V_r$. Analogamente poiché $y_0 \in V_r$ e vale anche $q_{ij}([y_0]_{\sim_j}) = [y_0]_{\sim_i}$ si dimostra che $V_r \subseteq U_1$. Possiamo allora concludere che $U_1 = V_r$. Tale ragionamento si può ripetere per ogni insieme di i che sarà uguale ad un insieme di j e poiché i e j sono finiti ed hanno lo stesso numero di elementi i e j devono essere uguali.
Dimostriamo che I è diretto. Siano $i, j \in I$, $i = \{U_1, \ldots, U_m\}$, $j = \{V_1, \ldots V_n\}$ e definiamo

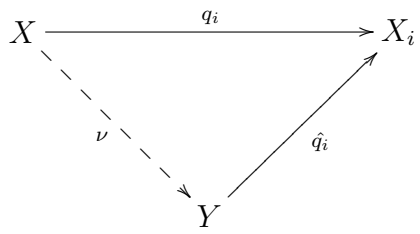
$$k := \{U_r \cap V_s \text{ con } 1 \leq r \leq m \text{ e } 1 \leq s \leq n\} \in I.$$

Gli spazi $U_r \cap V_s$ sono aperti, chiusi e disgiunti poiché gli spazi U_r e gli spazi V_s lo sono. Inoltre

$$(U_1 \cap V_1) \cup (U_1 \cap V_2) \cup \ldots \cup (U_1 \cap V_n) \cup \ldots \cup (U_m \cap V_1) \cup (U_m \cap V_2) \cup \ldots \cup (U_m \cap V_n) =$$

$$= U_1 \cap (\bigcup_{s=1}^{n} V_s) \cup \ldots \cup U_m \cap (\bigcup_{s=1}^{n} V_s) = U_1 \cup \ldots \cup U_m = X.$$

Si ha che $i \leq k$ poiché basta prendere la mappa q_{ik} tale che $q_{ik}([x]_{\sim_k}) = [x]_{\sim_i}$, che è ben definita per come è definito k e analogamente si ha che $j \leq k$. Allora I è diretto.
Proviamo che (X_i, q_{ij}) è un sistema inverso. Dobbiamo mostrare che per $i \leq k \leq j$ si ha $q_{ik} = q_{ij} \circ q_{jk}$ cioè dobbiamo far vedere che per ogni $x^k \in X_k$ si ha che $q_{ik}(x^k) = q_{ij} \circ q_{jk}(x^k)$. Poiché q_k è suriettiva esiste $x \in X$ tale che $x^k = q_k(x)$ allora $q_{ik}(q_k(x)) = (q_{ij} \circ q_{jk})(q_k(x))$ poiché per definizione $q_{ik} \circ q_k = q_i$, $q_{jk} \circ q_k = q_j$ e $q_{ij} \circ q_j = q_i$.
Sia $Y =: \varprojlim X_i$ con mappe $\hat{q}_i : Y \longrightarrow X_i$.
Le q_i sono compatibili per come sono definite le q_{ij} e quindi per la proprietà universale del limite inverso esiste $\nu : X \longrightarrow Y$ continua tale che $\hat{q}_i \circ \nu = q_i$ per ogni i.



Se dimostriamo che Y è un omeomorfismo per l'Osservazione 3.2 abbiamo dimostrato la tesi del teorema. Poiché gli X_i sono discreti e quindi di Hausdorff, Y è di Haudorff per la Proposizione 3.3. Inoltre X è quasi compatto per ipotesi e ν è continua, quindi basta dimostrare ν è biunivoca per poter affermare che ν è un omeomorfismo.
Dimostriamo ora che ν è iniettiva, siano dunque x_1, $x_2 \in X$ tali che $\nu(x_1) = \nu(x_2)$. Per ogni i si ha quindi che $\hat{q}_i(\nu(x_1)) = \hat{q}_i(\nu(x_2))$ dunque $q_i(x_1) = q_i(x_2)$ per ogni i quindi se U_r è l'insieme della partizione i tale che $x_1 \in U_r$ allora anche $x_2 \in U_r$.
Per il Lemma 1.4 punto 2 abbiamo che $\bigcap \{S$ tale che S è chiuso e aperto di X e $x_1 \in S\}$ è connesso, ma $x_2 \in S$ per ognuno di tali S: poiché $\{X \setminus S, S\}$ è una partizione di X di aperti e chiusi ha quindi associato un indice $k \in I$ e quindi $q_k(x_1) = q_k(x_2)$. Allora x_1, $x_2 \in \bigcap_{x_1 \in S} \{S$ tale che S è chiuso e aperto di $X\}$, ma X è totalmente disconnesso quindi $x_1 = x_2$ e quindi ν è iniettiva.
Dimostriamo ora che ν è suriettiva. Poiché $\hat{q}_i(\nu(X)) = q_i(X) = X_i$ per ogni i allora per la Proposizione 3.4 punto 3 si ha che $\nu(X)$ è denso in Y quindi $\overline{\nu(X)} = Y$. Essendo ν continua e X quasi compatto si ha che $\nu(X)$ è quasi compatto, ma $\nu(X) \subseteq Y$ che come

abbiamo già notato è di Hausdorff, allora $\nu(X)$ è chiuso in Y. Allora $\nu(X) = \overline{\nu(X)} = Y$ e quindi ν è suriettiva.
Per quanto precedentemente affermato possiamo dunque concludere che ν è un omeomorfismo e che quindi X è il limite inverso dei suoi spazi quoziente.

□

Capitolo 4

Gruppi profiniti

L'interesse nello studio dei gruppi profiniti nasce inizialmente dalla studio dei gruppi di Galois di estensioni di campi di Galois infinite. Furono chiamati in un primo tempo 'gruppi di tipo Galois'. Il termine 'gruppo profinito' fu introdotto per la prima volta probabilmente da Serre con il significato di 'limite proiettivo di gruppi finiti'. Alcuni gruppi profiniti erano conosciuti già dalla fine del '800, ad esempio il gruppo degli interi p-adici fu definito da Hensel nel 1899. Fu di Krull nel 1928 l'idea di dotare i gruppi di Galois di una topologia, ma solo nel 1955 fu provato da Leptin per la prima volta che ogni gruppo profinito è isomorfo ad un gruppo di Galois. La prima esposizione esaustiva della teoria dei gruppi profiniti comparve nel libro 'Cohomologie Galoisienne' di Serre nel 1964. Attualmente sono oggetto di ricerca in diverse aree della matematica come l'Analisi, la Teoria dei Gruppi e la Teoria dei Numeri.

Proposizione 4.1. *Sia (G_i, φ_{ij}) un sistema inverso di gruppi topologici indicizzato da I con G_i quasi compatto e di Haudorff per ogni i. Sia (G, φ_i) il limite inverso di (G_i, φ_{ij}). Sia L un sottogruppo normale di G aperto, allora*

a) esiste $i \in I$ tale che $\ker \varphi_i$ è un sottogruppo chiuso di L.

b) Il gruppo topologico G/L è isomorfo come gruppo toplogico ad un gruppo quoziente di un sottogruppo di qualche G_i.

c) Se inoltre ogni mappa φ_i è suriettiva allora G/L è isomorfo ad un gruppo quoziente di qualche G_i.

Dimostrazione. Ricordiamo che per ipotesi la mappa $\varphi_i : G \longrightarrow G_i$ è un omomorfismo continuo per ogn i. Per la Proposizione 3.4 punto 2 sappiamo che una base per G è data dall'insieme $\{\varphi_i^{-1}(U^i)$, con $i \in I$ e U^i aperti di $G_i\}$. Allora L è unione di aperti del tipo

$\varphi_i^{-1}(U^i)$ e almeno uno di questi deve contenere $1_G \in L$. Esistono dunque $k \in I$ e U^k aperto di X_k tale che $1_G \in \varphi_k^{-1}(U^k)$. Ma

$$L \supseteq \varphi_k^{-1}(U^k) = \{g \in G \text{ tali che } \varphi_k(g) \in U^k\} \supseteq \{g \in G \text{ tali che } \varphi_k(g) = 1_G\} = \ker \varphi_k,$$

dunque $\ker \varphi_k$ è un sottogruppo di G contenuto in L.

a) Proviamo ora che $\ker \varphi_k$ è chiuso in L. Chiaramente $\ker \varphi_k = \varphi_k^{-1}(1_{G_k})$. Poiché G_k è di Hausdorff per la Proposizione 2.2 punto f) 1_{G_k} è un chiuso di G_k ed essendo φ_k continua si ha che $\ker \varphi_k$ è un chiuso di G. Quindi $\ker \varphi_k$ è anche un chiuso di L.

b) Per il terzo teorema di isomorfismo fra gruppi topologici $(G/\ker \varphi_k)/(L/\ker \varphi_k)$ è isomorfo come gruppo topologico a G/L. Poiché i gruppi topologici G_i sono quasi compatti e di Hausdorff per la Proposizione 3.3 punto 4 si ha che G è quasi compatto. Inoltre $\varphi_k(G)$ è di Hausdorff poiché contenuto in G_k che è di Hausdorff. Per il primo teorema di isomorfismo per gruppi topologici 2.3 esiste un isomorfismo di gruppi topologici f fra $G/ker\varphi_k$ e $\varphi_k(G)$. Per il Lemma 2.6 con $C = L/\ker \varphi_k$, si ha che G/L è isomorfo come gruppo topologico a $\varphi_k(G)/(f(L/\ker \varphi_k))$ e quindi G/L è isomorfo ad un gruppo quoziente di un sottogruppo di G_k cioè $\varphi_k(G)$.

c) Se le mappe φ_i sono suriettive per ogni i allora $\varphi_k(G) = G_k$ e quindi G/L è isomorfo ad un gruppo quoziente di G_k.

□

Definizione 4.1. Sia G un gruppo e sia I una famiglia di sottogruppi normali di G. La famiglia I è detta base filtro se per ogni $K_1, K_2 \in I$ esiste $K_3 \in I$ tale che $K_3 \subseteq K_1 \cap K_2$.

Proposizione 4.2. *Sia G un gruppo topologico e I una base filtro di sottogruppi normali di G chiusi.*
Definiamo la relazione $\leq'$ in I in questo modo se $K, L \in I$, si ha $K \leq' L$ se e solo se $L \leq K$. Valgono dunque le seguenti affermazioni.

1. *L'insieme parzialmente ordinato $(I, \leq')$ è diretto e gli omomorfismi suriettivi definiti per $K \leq' L$*

$$\begin{array}{rccc} q_{KL}: & G/L & \longrightarrow & G/K \\ & gL & \longmapsto & gK \end{array}$$

   rendono $(G/K, q_{KL})$ indicizzato da I un sistema inverso.

2. *Poniamo $\hat{G} := \varprojlim G/K$. Esiste un omomorfismo continuo $\theta : G \longrightarrow \hat{G}$ tale che $\ker \theta = \bigcap_{K \in I} K$, l'immagine di θ è un sottogruppo denso di $\hat{G}$ e $\varphi_K \circ \theta$ è la mappa quoziente da G a G/K per ogni $K \in I$.*

3. *Se G è quasi compatto allora θ è suriettiva. Se G è quasi compatto e $\bigcap_{K\in I} K = 1_G$ allora θ è un isomorfismo di gruppi topologici e quindi G è isomorfo come gruppo topologico a $\varprojlim G/K$.*

Dimostrazione. 1. Per dimostrare che I è diretto occorre far vedere che se $K, L \in I$ allora esiste $M \in I$ tale che $M \leq' K$ e $M \leq' L$. Poiché I è una base filtro esiste $M \in I$ tale che M è un sottogruppo sia di K che di L. Inoltre M è un chiuso di G e quindi è anche un chiuso di K e L dotati della topologia indotta. Il resto della dimostrazione è analoga all'esempio 6.

2. Proviamo l'affermazione prima per $\hat{G} = s\varprojlim G/K$. Sia ha che

$$\hat{G} = \{c \in \prod_{K\in I} G/K \text{ tali che } q_{UV} \circ p_V(c) = p_U(c) \text{ per ogni } U, V \in I \text{ con } U \leq' V\},$$

dove le mappe $p_V : \prod_{K\in I} G/K \longrightarrow G/V$ sono proiezioni.
Definiamo la mappa

$$\begin{array}{rccc} \bar{\theta}: & G & \longrightarrow & \prod_{K\in I} G/K \\ & g & \longmapsto & (gK)_{K\in I} \end{array}$$

La mappa $\bar{\theta}$ è continua poiché per ogni $U \in I$ si ha che $p_U \circ \bar{\theta}$ è continua, infatti per ogni $U \in I$, per ogni $g \in G$ si ha che $p_U \circ \bar{\theta}(g) = gU = p_U(g)$ e la mappa p_U è continua. Proviamo che $\bar{\theta}(G) \subseteq \hat{G}$ cioè che per ogni $g \in G$ e per ogni $U \leq' V$ si ha che $q_{UV} \circ p_V((gK)_{K\in I}) = p_U((gK)_{K\in I})$, che risulta essere vero poiché $p_U((gK)_{K\in I}) = gU$ e $q_{UV} \circ p_V((gK)_{K\in I}) = q_{UV}(gV)$.
Sia

$$\begin{array}{rccc} \theta: & G & \longrightarrow & \hat{G} \\ & g & \longmapsto & (gK)_{K\in I} \end{array}$$

Poiché in $\hat{G}$ è presente per definizione la topologia indotta e poiché abbiamo provato che $\bar{\theta}$ è continua si ha che anche θ è continua. La mappa θ è chiaramente un omomorfismo di gruppi e inoltre per ogni $U \in I$ si ha che $\varphi_U \circ \theta$ è la mappa quoziente da G a G/U poiché $\varphi_U = p_{U|\hat{G}}$ e abbiamo visto che $p_U \circ \bar{\theta} = p_U$.
Proviamo che $\ker\theta = \bigcap_{K\in I} K$. Si ha che $g \in \ker\theta$ se e solo se $\theta(g) = 1_{\hat{G}} = 1_{\prod G/K}$, se e solo se $gK = 1_G K$ per ogni $K \in I$, se e solo se $g \in K$ per ogni $K \in I$.
Proviamo che $\theta(G)$ è denso in $\hat{G}$: per ogni $U \in I$ si ha che $\varphi_U(\theta(G)) = p_U(G) = = G/U$, allora per la Proposizione 3.4 punto 3 si ha che $\theta(G)$ è denso in $\hat{G}$.

Dimostriamo ora che ciò che abbiamo provato vale anche per ogni altro limite inverso (G^*, φ_K^*). Per il Teorema 3.1 sappiamo che esiste un omeomorfismo $\bar{\varphi} : \hat{G} \longrightarrow G^*$ tale che $\varphi_K^* \circ \bar{\varphi} = p_{K|\hat{G}}$. Consideriamo $\theta^* := \bar{\varphi} \circ \theta$, che risulta dunque un omomorfismo di gruppi continuo.
Proviamo che $\ker \theta^* = \{g \in G \text{ tali che } \theta^*(g) = (\bar{\varphi} \circ \theta)(g) = 1_{G^*}\} = \bigcap_{K \in I} K$. Si ha che $(\bar{\varphi} \circ \theta)(g) = 1_{G^*}$ se e solo se $\theta(g) = 1_{\hat{G}}$ essendo $\bar{\varphi}$ un omomorfismo di gruppi iniettivo, se e solo se $g \in \bigcap_{K \in I} K$, per quanto già visto.
Proviamo che $\theta^*(G)$ è denso in G^*. Dobbiamo far vedere che $\overline{\theta(G)} \supseteq G^*$. Sia $g^* \in G^*$; se per assurdo esistesse un intorno U_{g^*} di g^* in G^* tale che $U_{g^*} \cap \theta^*(G) = \emptyset$ allora essendo $\bar{\varphi}$ biunivoca e poiché $(\bar{\varphi}^{-1} \circ \theta^*)(G) = \theta(G)$ si avrebbe che $\bar{\varphi}^{-1}(U_{g^*}) \cap \theta(G) = \emptyset$. Ma essendo $\bar{\varphi}$ continua $\bar{\varphi}^{-1}(U_{g^*})$ è un aperto di G^* contenente $\bar{\varphi}^{-1}(g^*)$ e quindi avremmo trovato un intorno di un elemento di $\hat{G}$ disgiunto da $\theta(G)$ che è assurdo.
Mostriamo infine che $\varphi_K^* \circ \theta^*(g) = gK$ per ogni $g \in G$ e per ogni $K \in I$. Si ha che

$$\varphi_K^* \circ \theta^*(g) = (p_{K|\hat{G}} \circ \bar{\varphi}^{-1}) \circ (\bar{\varphi} \circ \theta(g)) = p_{K|\hat{G}} \circ \theta(g) = gK.$$

3. Proviamo l'affermazione prima per $\hat{G} = s\varprojlim G/K$. Poiché per ogni $K \in I$ si ha che K è chiuso in G allora per l'Osservazione 2.2 punto f) lo spazio G/K è di Hausdorff per ogni $K \in I$. Dunque anche $\hat{G}$ è di Hausdorff per la Proposizione 3.3 punto 1. Se G è quasi compatto allora $\theta(G)$ è quasi compatto poiché θ è continua. Si ha quindi che $\theta(G)$ è un chiuso in $\hat{G}$. Per il precedente punto $\theta(G)$ è denso in $\hat{G}$ dunque $\theta(G) = \overline{\theta(G)} = \hat{G}$ e quindi θ è suriettiva.
Proviamo ora che se G è quasi compatto e $\bigcap_{K \in I} K = 1$ allora θ è un isomorfismo di gruppi topologici. Se $\bigcap_{K \in I} K = 1$ allora θ è una mappa iniettiva e quindi θ è un isomorfismo di gruppi da G in $\hat{G}$ continuo. Si ha però che G è quasi compatto per ipotesi e $\hat{G}$ è di Hausdorff allora θ è un isomorfismo di gruppi topologici.
Dimostriamo ora che ciò che abbiamo provato vale anche per ogni altro limite inverso (G^*, φ_K^*). Consideriamo θ^* definita come nel precedente punto della dimostrazione. Se G è quasi compatto allora θ^* è suriettiva poiché θ è suriettiva. Se G è quasi compatto e $\bigcap_{K \in I} K = 1_G$ allora θ è un omeomorfismo dunque anche θ^* lo è. Quindi θ^* risulta essere un isomorfismo di gruppi topologici.

□

Notazione. Per classe di gruppi finiti si intenderà una classe di gruppi finiti che è chiusa rispetto alle immagini isomorfe cioè tale che se F_1 appartiene alla classe e F_1 è isomorfo a F_2 allora anche F_2 appartiene alla classe.

Definizione 4.2. Sia $\mathcal{C}$ una classe di gruppi finiti, un gruppo F è detto $\mathcal{C}$-gruppo se $F \in \mathcal{C}$, un gruppo G è detto pro-$\mathcal{C}$ gruppo se G è il limite inverso di un sistema inverso di $\mathcal{C}$-gruppi.

Se non specificato diversamente si considererà un gruppo finito con la topologia discreta. Si noti che se $\mathcal{C}$ è una classe di gruppi finiti e se G_i sono pro-$\mathcal{C}$ gruppi per ogni i allora in generale non vale né che $\varprojlim G_i$ sia finito né che $\varprojlim G_i$ possieda la topologia discreta.

Definizione 4.3. Sia $\mathcal{C}$ una classe di gruppi finiti.
Si dirà che $\mathcal{C}$ è chiusa per sottogruppi se ogni sottogruppo di un $\mathcal{C}$-gruppo è un $\mathcal{C}$-gruppo.
Si dirà che $\mathcal{C}$ è chiusa per quozienti se ogni gruppo quoziente di un $\mathcal{C}$-gruppo è un $\mathcal{C}$-gruppo.
Si dirà che $\mathcal{C}$ è chiuso per prodotto diretto se per ogni $F_1, F_2 \in \mathcal{C}$ si ha che anche $F_1 \times F_2 \in \mathcal{C}$.

Alcune classi importanti sono la classe di tutti i gruppi finiti, se p è un numero primo fissato la classe di tutti i gruppi il cui ordine è una potenza di p (detti p-gruppi finiti) e la classe di tutti i gruppi finiti ciclici.

Definizione 4.4. Un gruppo profinito è un pro-$\mathcal{C}$ gruppo dove $\mathcal{C}$ è la classe di tutti i gruppi finiti. Cioè un gruppo profinito è il limite inverso di un sistema inverso di gruppi finiti.

Osservazione 4.3. *Un $\mathcal{C}$-gruppo G è un pro-$\mathcal{C}$ gruppo.*

Dimostrazione. Sia $I = \{i\}$ e $G_i := G$. Risulta chiaro che $(I, \subseteq)$ è un insieme diretto parzialmente ordinato. Consideriamo (G_i, φ_{ij}) indicizzato da I, con $\varphi_{ii} = id_G$. Chiaramente (G_i, φ_{ij}) risulta un sistema inverso. Si ha dunque che

$$s\varprojlim G_i = \{x \in G \text{ tali che } \varphi_{ii}(p_i(x)) = p_i(x)\} = G.$$

Le mappe di tale limite inverso sono $\varphi_i = p_{i|G} = p_i = id_G$.

□

Esempio 7. *Un pro-$\mathcal{C}$ gruppo non è necessariamente un $\mathcal{C}$-gruppo.*

Dimostrazione. Consideriamo ad esempio il sistema inverso dell'esempio 5 del capitolo 3 ovvero $(\mathbb{Z}_{p^i}, \varphi_{ij})$ con $\varphi_{ij}([x]_{p^j}) = [x]_{p^i}$. Si ha che

$$s\varprojlim \mathbb{Z}_{p^i} = \{([a_k]_{p^k})_{k\in\mathbb{N}} \in \prod_{k=1}^{\infty} \mathbb{Z}_{p^k} \text{ t.c. } [a_j]_{p^i} = \varphi_{ij}([a_j]_{p^j}) = [a_i]_{p^i} \text{ per ogni } i, j \text{ con } j \geq i\}.$$

Quindi $s\varprojlim \mathbb{Z}_{p^i}$ è un gruppo profinito, mostriamo che però non è finito. Per ogni $s \in \mathbb{N}$ si ha che $([s]_{p^k})_{k\in\mathbb{N}} \in s\varprojlim \mathbb{Z}_{p^i}$. Inoltre se $s_1, s_2 \in \mathbb{N}$ e $s_1 \neq s_2$ allora $([s_1]_{p^k})_{k\in\mathbb{N}} \neq ([s_2]_{p^k})_{k\in\mathbb{N}}$ altrimenti p^k dividerebbe $s_1 - s_2$ per ogni $k \in \mathbb{N}$.

□

Teorema 4.4. *Sia $\mathcal{C}$ una classe di gruppi finiti chiusa per sottogruppi e per prodotti diretti e sia G un gruppo topologico. Sono equivalenti:*

1. *G è un gruppo pro-$\mathcal{C}$.*
2. *G è isomorfo come gruppo topologico ad un sottogruppo chiuso di un prodotto cartesiano di $\mathcal{C}$-gruppi.*
3. *G è quasi compatto e $\bigcap\{N \text{ tali che } N \lhd_O G \text{ e } G/N \in \mathcal{C}\} = 1_G$.*
4. *G è quasi compatto e totalmente disconnesso e per ogni $L \lhd_O G$ esiste $N \lhd_O G$ con $N \leq L$ e $G/N \in \mathcal{C}$.*

Se inoltre $\mathcal{C}$ è chiuso per quozienti allora il punto 4 può essere sostituito da

4'. *G è quasi compatto e totalmente disconnesso, e $G/L \in \mathcal{C}$ per ogni $L \lhd_O G$.*

Dimostrazione. $1 \Rightarrow 2$. Se G è un limite inverso di gruppi topologici $G_i \in \mathcal{C}$ allora G è isomorfo come gruppo topologico a $s\varprojlim X_i$. Per la Proposizione 3.3 punto 3, poiché gli spazi G_i sono di Hausdorff per ogni i (essendo discreti per ogni i) si ha che $s\varprojlim G_i$ è un sottogruppo chiuso del prodotto cartesiano $\prod_{i\in I} G_i$.

$2 \Rightarrow 3$. Sia G isomorfo come gruppo topologico ad un sottogruppo chiuso $\hat{G}$ di $\prod_{i\in I} G_i$ con $G_i \in \mathcal{C}$.
Proviamo che G è quasi compatto. Si faccia attenzione che anche se in G_i è presente la topologia discreta in generale la topologia prodotto in $\prod_{i\in I} G_i$ non coincide con la topologia discreta. I gruppi G_i se considerati con la topologia discreta sono anche gruppi topologici e sono dunque chiaramente quasi compatti. Allora anche $\prod_{i\in I} G_i$ è quasi compatto quindi anche $\hat{G}$, essendo chiuso, è quasi compatto. Si ha allora che anche G è quasi compatto poiché isomorfo come gruppo topologico a $\hat{G}$.
Proviamo che $\bigcap\{M \text{ tali che } M \lhd_O G \text{ e } G/M \in \mathcal{C}\} = 1_G$.
Per ogni $k \in I$ definiamo $N_k := \ker p_k \cap \hat{G}$ dove $p_k : \prod_{i\in I} G_i \longrightarrow G_k$ è la mappa proiezione. Proviamo che $N_k \lhd_O \hat{G}$ per ogni k, che $\bigcap_{i\in I} N_i = 1$ e che $\hat{G}/N_k \in \mathcal{C}$ per ogni k.
Poiché 1_{G_k} è aperto per la topologia discreta in G_k per ogni k, allora si ha che $\ker p_k = p_k^{-1}(1_{G_k})$ è aperto per la topologia prodotto in $\prod_{i\in I} G_i$, quindi N_k è aperto

in $\hat{G}$ per la topologia indotta dalla topologia prodotto per ogni k.
Poiché $\ker p_i$ è normale in $\prod_{i\in I} G_i$ e $\hat{G}$ è un sottogruppo di $\prod_{i\in I} G_i$ per il Teorema 2.4, si ha che $\ker p_i \cap \hat{G}$ è un sottogruppo normale di $\hat{G}$.
Per definizione di proiezione e di $1_{\prod G_i}$ si ha che $\bigcap_{i\in I} \ker p_i = 1_{\prod G_i}$. Ma $N_i \subseteq \ker p_i$ per ogni i allora $\bigcap_{i\in I} N_i \subseteq \bigcap_{i\in I} \ker p_i = 1_{\prod G_i}$.
Proviamo che $\hat{G}/N_i \in \mathcal{C}$ per ogni i. Mostriamo prima che $\hat{G}/(\hat{G}\cap \ker p_i)$ è isomorfo come gruppo topologico a $\hat{G}\ker p_i/\ker p_i$. Dato che $\ker p_i = \ker p_i \cap \hat{G}\ker p_i$ e $\ker p_i$ è un chiuso di G si ha che $\ker p_i$ è un chiuso di $\hat{G}\ker p_i$ e quindi $\hat{G}\ker p_i/\ker p_i$ è di Hausdorff per l'Osservazione 2.2 punto f). Per il secondo teorema di isomorfismo per gruppi topologici 2.4, dato che $\hat{G}$ è quasi compatto, si ha che $\hat{G}/(\hat{G}\cap \ker p_i)$ è isomorfo come gruppo topologico a $(\hat{G}\ker p_i)/\ker p_i$.
Tenendo presente che $\ker p_i$ è normale in $\prod_{i\in I} G_i$ per ogni i si verifica facilmente che $\hat{G}\ker p_i$ è un sottogruppo di $\prod_{i\in I} G_i$ contenente $\ker p_i$ per ogni i (ad esempio se $\hat{g} \in \hat{G}$ e $k^i \in \ker p_i$ allora $(gk^i)^{-1} = k^{i^{-1}}g^{-1} = g^{-1}k^{i'}$ con $k^{i'} \in \ker p_i$) e quindi $\hat{G}\ker p_i/\ker p_i$ è un sottogruppo di $\prod_{i\in I} G_i/\ker p_i$ per ogni i.
Poiché $\prod_{k\in K} G_k$ è quasi compatto, G_i è di Hausdorff per ogni i e p_i è continua per ogni i, per il primo teorema di isomorfismo per gruppi topologici 2.3 si ha che $\prod_{k\in K} G_k/\ker p_i$ è isomorfo come gruppo topologico a G_i. Allora per ogni i si ha $\hat{G}/N_i = \hat{G}/(\hat{G}\cap \ker p_i) \cong \hat{G}\ker p_i/\ker p_i$ il quale è un sottogruppo di $\prod_{k\in K} G_k/\ker p_i \cong G_i$. Poiché $\mathcal{C}$ per ipotesi è chiuso per isomorfismi e per sottogruppi e $G_i \in \mathcal{C}$ per ogni i si ha che $\hat{G}/N_i \in \mathcal{C}$ per ogni i.
Se $x \in N$ per ogni $N \triangleleft_O G$ con N tale che $G/N \in \mathcal{C}$, allora in particolare $x \in N_i$ per ogni i e quindi $\bigcap\{N \text{ tali che } N\triangleleft_O \hat{G} \text{ e } \hat{G}/N \in \mathcal{C}\} \subseteq \bigcap_{i\in I} N_i = 1_G$.
Per ipotesi esiste un isomorfismo f di gruppi topologici da $\hat{G}$ in G. Poiché f è iniettiva si ha che $\bigcap_{i\in I} f(N_i) = f(\bigcap_{i\in I} N_i) = 1_G$. Inoltre $f(N_i)\triangleleft_O G$ e per il Lemma 2.6 si ha che $G/f(N_i) \cong \hat{G}/N_i \in \mathcal{C}$ per ogni i. Possiamo allora concludere che

$$\bigcap\{M \text{ tali che } M\triangleleft_O G \text{ e } G/M \in \mathcal{C}\} \subseteq \bigcap_{i\in I} f(N_i) = 1_{\hat{G}}.$$

$3 \Rightarrow 1$. Vogliamo utilizzare la Proposizione 4.2. Sia $I = \{N \text{ tali che } N \triangleleft_O G \text{ e } G/N \in \mathcal{C}\}$, proviamo che è una base filtro.
Si noti che se $N \triangleleft_O G$ la topologia quoziente su G/N coincide con quella discreta infatti: $gN \in G/N$ è un aperto per la topologia quoziente se la sua retroimmagine tramite la mappa quoziente è un aperto in G, che risulta essere vero per la Proposizione 2.2 punto b).
Siano $N_1, N_2 \in I$ consideriamo la mappa

$$\begin{array}{rccc} \psi: & G & \longrightarrow & G/N_1 \times G/N_2 \\ & g & \longmapsto & (gN_1, gN_2). \end{array}$$

Si ha che $G/N_1 \times G/N_2 \in \mathcal{C}$ poiché $G/N_1, G/N_2 \in \mathcal{C}$ per ipotesi. Per $i \in \{1,2\}$ siano $p_i : G/N_1 \times G/N_2 \longrightarrow G/N_i$ le proiezioni e $\pi_{N_i} : G \longrightarrow G/N_i$ le mappe quoziente. Risulta chiaro che ψ è un omomorfismo di gruppi e ψ è continua poiché $p_1 \circ \psi = \pi_{N_1}$ e $p_2 \circ \psi = \pi_{N_2}$. Inoltre $\ker \psi = \{g \in G \text{ tali che } g_1N_1 = N_1 \text{ e } g_2N_2 = N_2\} = N_1 \cap N_2$. Poiché $\psi(G)$ è un sottogruppo di $G/N_1 \times G/N_2$ allora $\psi(G) \in \mathcal{C}$. La mappa ψ è aperta poiché sia in G/N_1 che in G/N_2 è presente la topologia discreta e quindi in $G/N_1 \times G/N_2$ la topologia prodotto coincide con quella discreta. Per il primo teorema di isomorfismo dunque $G/\ker\psi$ è isomorfo come gruppo topologico a $\psi(G) \in \mathcal{C}$ allora $G/(N_1 \cap N_2) \in \mathcal{C}$. Inoltre risulta chiaro che $N_1 \cap N_2$ è un aperto normale di G allora $N_1 \cap N_2 \in I$. Si è provato quindi che I è una base filtro. Allora per la Proposizione 4.2 $(G/N, q_{NM})_{\substack{N,M \in I \\ N \leq' M}}$ con

$$\begin{array}{rccc} q_{NM}: & G/M & \longrightarrow & G/N \\ & gM & \longmapsto & gN \end{array}$$

è un sistema inverso. Se $\hat{G}$ è il limite inverso di tale sistema inverso, $\hat{G}$ risulta essere un gruppo pro-$\mathcal{C}$. Poiché per le ipotesi iniziali G è quasi compatto e $\bigcap_{N \in I} N = 1_G$ sempre per la Proposizione 4.2 si ha che $\hat{G}$ è isomorfo come gruppo topologico a G. Per l'Osservazione 3.2 abbiamo concluso.

$1 \Rightarrow 4$. Sia (G_i, φ_i) un sistema inverso, con $G_i \in \mathcal{C}$ per ogni $i \in I$, tale che $G = \varprojlim G_i$. Poiché ogni G_i è finito ed è dotato della topologia dicreta allora ogni G_i è quasi compatto, totalmente disconnesso e di Hausdorff. Per la Proposizione 3.3 punti 2 e 4 si ha che G è totalmente disconnesso e quasi compatto. Sia $L \triangleleft_O G$ proviamo che esiste $N \triangleleft_O G$ con $N \leq L$ tale che $G/N \in \mathcal{C}$. Per la Proposizione 4.1 esiste $k \in I$ tale che $\ker\varphi_k \leq L$. Prendiamo $N = \ker\varphi_k$. Chiaramente $\ker\varphi_k \triangleleft_O G$. Si ha che φ_k è aperta poiché il suo codomonio, G_k, è discreto. Dunque, essendo φ_k anche continua, si ha che $G/\ker\varphi_k \cong \text{Im } \varphi_k$ come gruppi topologici. Dato che Im φ_k è un sottogruppo di $G_k \in \mathcal{C}$ si ha che $G/\ker\varphi_k \in \mathcal{C}$.

$4 \Rightarrow 3$. È chiaro che $\bigcap\{N \text{ tali che } N \triangleleft_O G\} \subseteq \bigcap\{N \text{ tali che } N \triangleleft_O G \text{ e } G/N \in \mathcal{C}\}$. Ma vale anche che $\bigcap\{N \text{ tali che } N \triangleleft_O G\} \supseteq \bigcap\{N \text{ tali che } N \triangleleft_O G \text{ e } G/N \in \mathcal{C}\}$; infatti se per assurdo esistesse $x \in N$ per ogni $N \triangleleft_O G$ con $G/N \in \mathcal{C}$ e $x \notin L$ per un qualche $L \triangleleft_O G$ allora per ipotesi esisterebbe $N' \triangleleft_O G$, $N' \leq L$ tale che $G/N' \in \mathcal{C}$. Allora si avrebbe che $x \in N' \subseteq L$ che è assurdo. Per la Proposizione 2.8 punto c) 3 possiamo concludere che $\bigcap\{N \text{ tali che } N \triangleleft_O G \text{ e } G/N \in \mathcal{C}\} = \bigcap\{N \text{ tali che } N \triangleleft_O G\} = 1_G$.

Poniamoci ora nel caso in cui $\mathcal{C}$ è chiuso anche per quozienti e proviamo che i punti 4 e 4' sono equivalenti.

$4' \Rightarrow 4$. Sia $L \triangleleft_O G$ allora chiaramente $L \leq L$ e per ipotesi $G/L \in \mathcal{C}$.

$4 \Rightarrow 4'$. Sia $L \triangleleft_O G$, proviamo che $G/L \in \mathcal{C}$. Abbiamo già provato che esistono $G_i \in \mathcal{C}$ tali che $G = \varprojlim G_i$ con mappe del limite inverso φ_i. Per la Proposizione 4.1 esiste $k \in I$ tale che $\ker \varphi_k \leq L$. Poiché φ_k è aperta per il primo teorema di isomorfismo fra gruppi topologici si ha che $G/\ker \varphi_k \cong \varphi_k(G) \in \mathcal{C}$. Ma per il terzo teorema di isomorfismo per gruppi topologici 2.5 si ha che $G/L \cong (G/\ker \varphi_k)/(L \ker \varphi_k) \in \mathcal{C}$.

□

Corollario 4.5. *Sia G un gruppo topologico. Sono equivalenti:*

1. *G è un gruppo profinito.*
2. *G è isomorfo come gruppo topologico ad un sottogruppo chiuso di un prodotto cartesiano di gruppi finiti.*
3. *G è quasi compatto e $\bigcap\{N \text{ tali che } N \triangleleft_O G\} = 1_G$.*
4. *G è quasi compatto e totalmente disconnesso.*

Dimostrazione. Consideriamo $\mathcal{C}$ la classe di tutti i gruppi finiti, che risulta essere chiusa per isomorfismi, per sottogruppi, per prodotti diretti e per quozienti. I punti 3 e 4 derivano dal fatto che $\mathcal{C}$ è chiuso per quozienti.

□

Teorema 4.6. *Sia G un gruppo profinito. Se I è una base filtro di sottogruppi normali chiusi di G tali che $\bigcap_{N \in I} N = 1_G$ allora*

1. *$G \cong \varprojlim_{N \in I} (G/N)$*
2. *$H \cong \varprojlim_{N \in I} (H/H \cap N)$ per ogni sottogruppo chiuso H di G.*
3. *$G/K \cong \varprojlim_{N \in I} (G/KN)$ per ogni sottogruppo normale chiuso K di G.*

Si noti che i punti 2 e 3 valgono anche per ogni sottogruppo aperto di G per la 2.2 punto c). Si osservi inoltre che ad esempio $I = \{N \text{ tali che } N \triangleleft_O G\}$ è chiaramente una base filtro di G ed è tale che $\bigcap_{N \triangleleft_O G} N = 1$ per la Proposizione 2.8.

Dimostrazione. 1. Poiché G è quasi compatto e $\bigcap_{N \in I} N = 1_G$, per la Proposizione 4.2 punto 3 si ha che $G \cong \varprojlim_{N \in I} (G/N)$.

2. Sia H un sottogruppo chiuso di G, consideriamo $J := \{H \cap N \text{ tali che } N \in I\}$. Poiché per ogni $N \in I$ si ha che N è un sottogruppo normale di G per il Teorema 2.4 si ha che $N \cap H$ è normale in H per ogni $N \in I$. Si ha anche che per ogni $N \in I$ vale che $H \cap N$ è un chiuso di H poiché N è un chiuso di G. Inoltre dati $H \cap N_1, H \cap N_2 \in J$ si ha che $(H \cap N_1) \cap (H \cap N_2) = H \cap (N_1 \cap N_2)$ e poiché esiste $N_3 \in I$ tale che $N_3 \subseteq N_1 \cap N_2$ si ha che $H \cap N_3 \subseteq H \cap (N_1 \cap N_2)$. Dunque J è una base filtro di sottogruppi normali di H chiusi.
Inoltre vale che $\bigcap_{L \in J} L = \bigcap_{N \in I} (N \cap H) \subseteq \bigcap_{N \in I} N = 1_G$. Si ha che H e quasi compatto poiché è chiuso in G e G è quasi compatto. Quindi per la Proposizione 4.2 punto 3 si ha che $H \cong \varprojlim_{L \in J} (H/L) = \varprojlim_{N \in I} (H/H \cap N)$.

3. Sia K un sottogruppo normale chiuso di G. Sia $J := \{KN \text{ tali che } N \in I\}$. Analogamente al punto 2 di questa dimostrazione si dimostra che J è una base filtro. Per ogni $N \in I$ si ha che KN è normale in G. Inoltre KN è chiuso in G. Infatti K e N sono chiusi in G e G è quasi compatto e di Hausdorff, quindi per la Proposizione 2.2 punto g) si ha che KN è un chiuso di G. Dunque J è una base filtro di sottogruppi normali chiusi di G.
Per ogni $N \in I$ si ha che $NK = KN$ dato che N è normale per ogni $N \in I$. Poiché per le ipotesi iniziali G è quasi compatto, I è una base filtro di chiusi di G e K è un chiuso di G possiamo utilizzare la Proposizione 2.2 punto h); dato che per le ipotesi iniziali vale anche $\bigcap_{N \in I} N = 1_G$ si ha

$$\bigcap_{M \in J} M = \bigcap_{N \in I} KN = (\bigcap_{N \in I} N)K = K.$$

Per la Proposizione 4.2 punto 3 si ha dunque che esiste un omomorfismo continuo $\theta : G \longrightarrow \varprojlim_{M \in J} G/M$ suriettivo con $\ker \theta = \bigcap_{M \in J} M = K$.
Poiché per ogni $M \in J$ si ha che M è chiuso in G allora per l'Osservazione 2.2 punto f) si ha che G/M è di Hausdorff per ogni $M \in J$ e quindi anche $\varprojlim_{M \in J} (G/M)$

lo è. Poiché G è quasi compatto per il primo teorema di isomorfismo per gruppi topologici si ha che $G/K \cong \varprojlim_{M\in J}(G/M) = \varprojlim_{N\in I}(G/KN)$.

□

Osservazione 4.7. *Sia $\mathcal{C}$ una classe di gruppi finiti chiusa per sottogruppi e prodotti diretti, allora*

1. *sottogruppi chiusi di gruppi pro-$\mathcal{C}$ sono gruppi pro-$\mathcal{C}$,*
2. *prodotti cartesiani di gruppi pro-$\mathcal{C}$ sono gruppi pro-$\mathcal{C}$,*
3. *limiti inversi di gruppi pro-$\mathcal{C}$ sono gruppi pro-$\mathcal{C}$,*

se inoltre $\mathcal{C}$ è chiuso per quozienti allora

4. *gruppi quozienti di gruppi pro-$\mathcal{C}$ tramite sottogruppi normali chiusi sono gruppi pro-$\mathcal{C}$.*

Dimostrazione. Sia G un pro-$\mathcal{C}$ gruppo.

1. Sia $H \leq G$. Per ipotesi esiste un isomorfismo di gruppi topologici f da G in $\hat{G}$ con $\hat{G} \leq \prod_{i\in I} G_i$ dove $G_i \in \mathcal{C}$. Proviamo che esiste $\hat{H} \leq \prod_{i\in I} G_i$ tale che H è isomorfo come gruppo topologico a $\hat{H}$. Prendiamo $\hat{H} = f(H)$. Si ha che H è isomorfo come gruppo topologico a $f(H)$. Inoltre $f(H) \leq \hat{G} \leq \prod_{i\in I} G_i$ dunque $f(H) \leq \prod_{i\in I} G_i$. Per il Teorema 4.4 punto 2 abbiamo concluso.

2. Siano G^i pro-$\mathcal{C}$ gruppi per ogni $i \in I$. Vogliamo provare che $\prod_{i\in I} G^i$ è un pro-$\mathcal{C}$ gruppo. Per ipotesi per ogni $i \in I$ esiste f^i isomorfismo di gruppi topologici da G^i a $\hat{G^i}$ con $\hat{G^i} \leq \prod_{j\in J_i} G^i_j$ dove $G^i_j \in \mathcal{C}$ per ogni $j \in J_i$.
   Proviamo che esiste un gruppo topologico M tale che $\prod_{i\in I} G^i \cong M \leq \prod_{l\in L} G_l$ con $G_l \in \mathcal{C}$ per ogni l. Poniamo $M = \prod_{i\in I} \hat{G^i}$. Si ha che $\prod_{i\in I} G^i \cong \prod_{i\in I} \hat{G^i}$ e si verifica facilmente che $\prod_{i\in I} \hat{G^i} \leq \prod_{i\in I}(\prod_{j\in J_i} G^i_j)$.

3. Siano G^i pro-$\mathcal{C}$ gruppi per ogni $i \in I$. Vogliamo provare che $\varprojlim G^i$ è un pro-$\mathcal{C}$ gruppo. Poiché i gruppi topologici G^i sono pro-$\mathcal{C}$, allora sono di Hausdorff, quindi per la Proposizione 3.3 punto 3 si ha che $s\varprojlim G^i$ è un sottogruppo chiuso di $\prod_{i\in I} G^i$.

Per il punto 2 di questa dimostrazione si ha che $\prod_{i\in I} G^i$ è un pro-$\mathcal{C}$ gruppo quindi esiste un gruppo topologico G^* tale che $\prod_{i\in I} G^i \cong G^* \leq \prod_{l\in L} G_l$, dove $G_l \in \mathcal{C}$. Sia f un isomorfismo di gruppi topologici da $\prod_{i\in I} G^i$ in G^*. Si ha che:

$$\varprojlim G^i \cong s\varprojlim G^i \cong f(s\varprojlim G^i) \leq G^* \leq \prod_{l\in L} G_l,$$

dunque $\varprojlim G^i \cong f(s\varprojlim G^i) \leq \prod_{l\in L} G_l$.

4. Se K è un sottogruppo normale chiuso di G e la classe $\mathcal{C}$ è chiusa per quozienti vogliamo provare che G/K è un pro-$\mathcal{C}$ gruppo. Poiché G è un pro-$\mathcal{C}$ gruppo si ha che G è quasi compatto e l'insieme $I := \{N \text{ tali che } N\triangleleft_O G \text{ con } G/N \in \mathcal{C}\}$ che per il Teorema 4.4 punto 4' è uguale a $\{N \text{ tali che } N\triangleleft_O G\}$ è una base filtro di G tale che $\bigcap_{N\in I} N = 1_G$. Per argomentazioni analoghe a quelle della dimostrazione del Teorema 4.6 punto 3, dove non si è mai sfruttato il fatto che $\mathcal{C}$ fosse la classe di tutti i gruppi finiti, si ha che $G/K \cong \varprojlim_{N\in I}(G/KN)$.
   Poiché $KN\triangleleft_O G$ e $\mathcal{C}$ è chiusa per quozienti per il Teorema 4.4 punto 4' si ha che $G/KN \in \mathcal{C}$ e quindi G/K è un pro-$\mathcal{C}$ gruppo.

□

Capitolo 5

Completamenti

Osservazione 5.1. *Sia G un gruppo e I una base filtro di sottogruppi normali di G, I non vuoto. Definiamo $\tau_0 := \{\bigcup_{j\in J} K_j g_j$ con $K_j \in I, g_j \in G\}$. Allora (G, τ_0) è un gruppo topologico.*

Dimostrazione. Proviamo prima che (G, τ_0) è uno spazio topologico.
Si ha che $\emptyset \in \tau_0$ e che $X \in \tau_0$ poiché $X = \bigcup_{g\in G} Kg$ se $K \in I$.
Proviamo che se $K_1, \ldots, K_n \in I$ e $g_1, \ldots, g_n \in G$ allora $K_1 g_1 \cap \ldots \cap K_n g_n \in \tau_0$. Se $\bigcap_{i=1}^{n} K_i g_i = \emptyset$ allora abbiamo concluso. Se invece esiste $x \in G$ tale che $x \in \bigcap_{i=1}^{n} K_i g_i$ allora per ogni i esiste $k_i \in K_i$ tale che $x = k_i g_i$. Dunque per ogni i si ha $K_i g_i = K_i x$. Allora

$$\emptyset \neq \bigcap_{i=1}^{n} K_i g_i = \bigcap_{i=1}^{n} K_i x = (\bigcap_{i=1}^{n} K_i)x$$

poiché se $y \in K_i x$ per ogni i allora esistono $k_i \in K_i$ tali che $y = k_1 x = \ldots = k_n x$ dunque $k_1 = \ldots = k_n$ quindi $y \in (\bigcap_{i=1}^{n} K_i)x$. Chiaramente $(\bigcap_{i=1}^{n} K_i)x \subseteq \bigcap_{i=1}^{n} K_i x$. Se $\bigcap_{i=1}^{n} K_i \in I$ abbiamo concluso. Se invece $\bigcap_{i=1}^{n} K_i \notin I$, poiché I è una base filtro esiste $K \in I$ tale che $K \subseteq \bigcap_{i=1}^{n} K_i$. Si ha quindi che $(\bigcap_{i=1}^{n} K_i)x = \bigcup\{Kgx$ tali che $g \in \bigcap_{i=1}^{n} K_i\}$. Infatti se G è un gruppo e H un suo sottogruppo si ha sempre che $G = \bigcup_{g\in G} Hg$ e se poniamo $G = \bigcap_{i=1}^{n} K_i$ e $H = K$ si ha che $\bigcap_{i=1}^{n} K_i = \bigcup\{Kg$ tali che $g \in \bigcap_{i=1}^{n} K_i\}$ da cui segue quanto voluto.

Dunque $\bigcap_{i=1}^{n} K_i x$ è unione di insiemi del tipo $K(gx)$ e quindi appartiene a τ_0.
L'unione di aperti di τ_0 è unione di unione di laterali e dunque unione di laterali.
Proviamo che (G, τ_0) è un gruppo topologico. Dobbiamo mostrare che le seguenti due mappe sono continue.

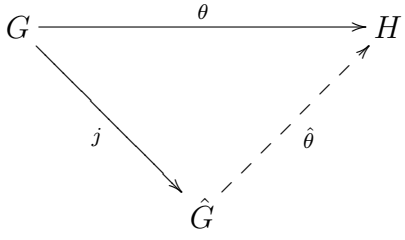
$$\begin{array}{rccc} \psi: & G & \longrightarrow & G \\ & g & \longmapsto & g^{-1} \end{array} \qquad \begin{array}{rccc} \chi: & G \times G & \longrightarrow & G \\ & (g_1, g_2) & \longmapsto & g_1 g_2. \end{array}$$

Per dimostrare che χ è continua basta provare che per ogni elemento Kx della base di τ_0 si ha che $\chi^{-1}(Kx) \in \mathcal{P}$. Mostriamo che $\chi^{-1}(Kx) = \bigcup_{g \in G} (Kxg^{-1} \times Kg)$. Se esistono $k_1, k_2 \in K$, $g \in G$ tali che $y = (k_1 x g^{-1}, k_2 g)$ allora $\chi(y) = k_1 x g^{-1} k_2 g \in Kx$ perché K è normale in G. D'altra parte se $g_1, g_2 \in G$ ed esiste $k \in K$ tale che $g_1 g_2 = kx$ allora $g_1 = k x g_2^{-1}$ quindi $(g_1, g_2) \in Kxg_2^{-1} \times Kg_2$.
Poiché $K \in I$ e $xg^{-1}, g \in G$ si ha che $K(xg^{-1}) \in \tau_0$ e $Kg \in \tau_0$, dunque $K(xg^{-1}) \times Kg \in \mathcal{P}$ e quindi anche $\bigcup_{g \in G} K(xg^{-1}) \times Kg \in \mathcal{P}$.
Per dimostrare che ψ è continua è sufficiente provare che per ogni $Kx \in \tau_0$ si ha che $\psi^{-1}(Kx) \in \tau_0$. Questo è vero poiché $\psi^{-1}(Kx) = Kx^{-1}$.

□

Notazione. Di seguito indicheremo con τ_0 la topologia data dall'insieme $\{\bigcup_{i \in I} K_i g_i \text{ con } K_i \in I, g_i \in G\}$.

Definizione 5.1. Siano G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Consideriamo il gruppo topologico (G, τ_0). Un completamento di G rispetto ad I consiste in un gruppo profinito $\hat{G}$ ed in un omomorfismo continuo fra gruppi topologici $j : G \longrightarrow \hat{G}$ tale che se H è un gruppo finito e $\theta : G \longrightarrow H$ è un omomorfismo continuo fra gruppi topologici allora esiste ed è unico un omomorfismo continuo $\hat{\theta} : \hat{G} \longrightarrow H$ tale che $\theta = \hat{\theta} \circ j$ ovvero tale che commuti il seguente diagramma.



Dato un gruppo G ed una base filtro non vuota di sottogruppi normali di G di indice finito dimostriamo ora che esiste sempre un completamento di G rispetto ad I.

Proposizione 5.2. *Siano G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Consideriamo G con la topologia τ_0. Sia $\hat{G} := \varprojlim_{K\in I} G/K$ e sia j la mappa definita nel seguente modo*

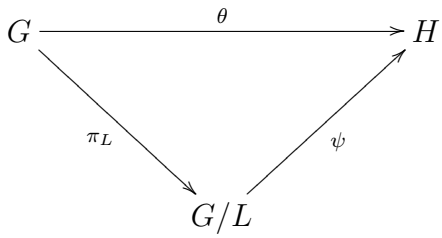
$$\begin{array}{rccc} j: & G & \longrightarrow & \hat{G} \\ & g & \longmapsto & (gK)_{K\in I} \end{array}$$

Allora $(\hat{G}, j)$ è un completamento di G rispetto a I.

Dimostrazione. Notiamo che $(G/K, q_{HK})$ è un sistema inverso poiché G è un gruppo topologico ed I è una base filtro di sottogruppi normali chiusi di G come richiesto dalla Proposizione 4.2. Notiamo anche che $j(G) \subseteq \hat{G} \subseteq \prod_{K\in I} G/K$ e che j è un omomorfismo continuo per la dimostrazione della Proposizione 4.2.
Siano H un gruppo finito e $\theta : G \longrightarrow H$ un omomorfismo continuo, proviamo che esiste ed è unico un omomorfismo continuo $\hat{\theta} : \hat{G} \longrightarrow H$ tale che $\theta = \hat{\theta} \circ j$.
Poiché in H consideriamo la topologia discreta $\ker\theta$ è un aperto di G. Si ha anche che $1_G \in \ker\theta$ dato che θ è un omomorfismo di gruppi. Esiste dunque $A \in \tau_0$ con $A \in 1_G$ tale che $A \subseteq \ker\theta$. Sia $A = \prod_{j\in J} K_j g_j$ con $K_j \in I$ e $g_j \in G$ per ogni j. Sia $K_l g_l$ contenente 1_G. Si ha che $K_l g_l = K_l$.
Poniamo $L := K_l \in I$. Chiaramente $L \subseteq \ker\theta$. Definiamo $\hat{\theta}$ la seguente composizione di due mappe.

$$\begin{array}{rccccc} \hat{\theta}: & \hat{G} & \longrightarrow & G/L & \longrightarrow & H \\ & (g_K K)_{K\in I} & \longmapsto & g_L L & \longmapsto & \theta(g_L). \end{array}$$

La prima mappa da sinistra è la proiezione p_L dal prodotto cartesiano dei gruppi topologici G/K in G/L ristretta a $\hat{G}$. La seconda mappa verrà chiamata ψ. Si noti che ψ è tale che il seguente diagramma sia commutativo.



Si ha che $\hat{\theta}$ è ben definita poiché ψ lo è: se $g_1, g_2 \in G$ e $g_1 g_2^{-1} \in L$ allora $\theta(g_1)\theta(g_2)^{-1} = 1_H$ poichè $L \subseteq \ker\theta$. Dunque $\psi(g_1 L) = \theta(g_1) = \theta(g_2) = \psi(g_2 L)$. Inoltre $\hat{\theta}$ è un omomorfismo di gruppi poiché p_L e θ lo sono. Si ha anche che $\hat{\theta}$ è continua, infatti la proiezione è continua poiché in $\hat{G}$ è presente la topologia indotta, ma anche ψ è continua poiché θ è continua.

Infine mostriamo che per ogni $g \in G$ si ha che $\theta(g) = (\hat{\theta} \circ j)(g)$. Si ha infatti che $(\hat{\theta} \circ j)(g) = \hat{\theta}((gK)_{K \in I}) = \psi(gL)$ per ogni $g \in G$.
Sia $\hat{\theta}' : \hat{G} \longrightarrow G$ un altro omomorfismo continuo tale che $\hat{\theta}' \circ j = \theta$. Consideriamo $Z := \{\hat{g} \in \hat{G}$ tali che $\hat{\theta}(\hat{g}) = \hat{\theta}'(\hat{g})\} \subseteq \hat{G}$. Si ha che Z è un chiuso poiché $\hat{\theta}, \hat{\theta}' : \hat{G} \longrightarrow H$ sono continue e H è di Hausdorff. Inoltre $j(G) \subseteq Z$ poiché $\hat{\theta} \circ j(g) = \theta(g) = \hat{\theta}' \circ j(g)$. Ma $\overline{j(G)} = \hat{G}$ come abbiamo già visto nella dimostrazione della Proposizione 4.2 punto 2. Poiché $j(G) \subseteq Z \subseteq \hat{G}$ si ha che $\hat{G} = \overline{j(G)} \subseteq \overline{Z} = Z$. Dunque $Z = \hat{G}$. Possiamo allora concludere che $\hat{\theta}(\hat{g}) = \hat{\theta}'(\hat{g})$ per ogni $\hat{g} \in \hat{G}$.

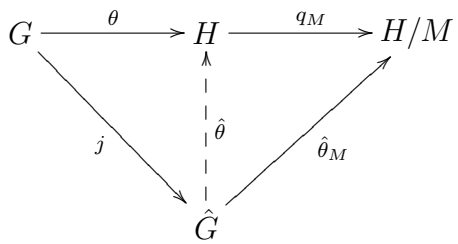
□

Proposizione 5.3. *Sia G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Consideriamo G con la topologia τ_0. Sia $\hat{G}$ un gruppo profinito e sia $j : G \longrightarrow \hat{G}$ un omomorfismo continuo. Sono equivalenti:*

a) $(\hat{G}, j)$ è un completamento di G rispetto a I.

b) Per ogni gruppo profinito H e per ogni omomorfismo continuo $\theta : G \longrightarrow H$ esiste ed è unico un omomorfismo continuo $\hat{\theta} : \hat{G} \longrightarrow H$ tale che $\hat{\theta} \circ j = \theta$.

Dimostrazione. Mostriamo prima che b) implica a). Basta osservare che se H è un gruppo finito allora H è quasi compatto e totalmente disconnesso, quindi H è un gruppo profinito.
Proviamo invece ora che a) implica b). Sia H un gruppo profinito e sia $\theta : G \longrightarrow H$ un omomorfismo continuo. Sia $M \triangleleft_O H$ e sia q_M la mappa quoziente da H in H/M.
Abbiamo che H è quasi compatto quindi per ogni $M \triangleleft_O H$ si ha che H/M è un gruppo finito. Poiché $q_M \circ \theta$ è un omomorfismo continuo per ipotesi esiste ed è unico un omomomorfismo continuo $\hat{\theta}_M$ tale che $\hat{\theta}_M \circ j = q_M \circ \theta$.
Consideriamo il seguente diagramma.



Abbiamo appena osservato che la parte esterna del diagramma è commutativa. Vogliamo provare che esiste un omomorfismo continuo $\hat{\theta}$ tale che la parte sinistra del diagramma sia commutativa.
Proviamo ora che la parte a destra del diagramma è commutativa per una opportuno omomorfismo continuo $\hat{\theta}$.

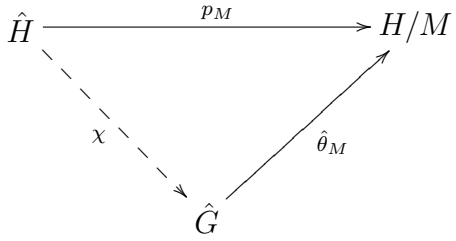
Per ogni $M \leq N$ con $M, N \triangleleft_O G$ consideriamo la mappa

$$\begin{array}{rccc} q_{NM}: & H/M & \longrightarrow & H/N \\ & hM & \longmapsto & hN. \end{array}$$

Poiché $\{M \triangleleft_O H\}$ è una base filtro di sottogruppi normali di H chiusi, per la Proposizione 4.2 si ha che $(H/M, q_{NM})$ è un sistema inverso.
Chiaramente si ha che $q_N = q_{NM} \circ q_M$. Mostriamo ora che le mappe $\hat{\theta}_M$ sono compatibili con il sistema inverso $(H/M, q_{MN})$ indicizzato dall'insieme degli $M \triangleleft_O H$. Si ha che per ogni $M \leq N$

$$q_{NM} \circ \hat{\theta}_M \circ j = q_{NM} \circ (q_M \circ \theta) = q_N \circ \theta = \hat{\theta}_N \circ j.$$

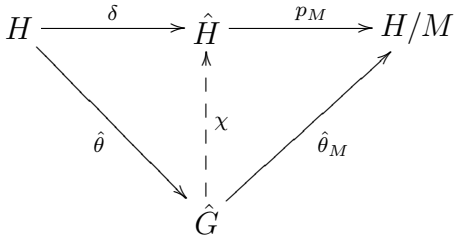
Dunque per l'unicità della mappe $\hat{\theta}_N$ si ha che $q_{NM} \circ \hat{\theta}_M = \hat{\theta}_N$ per ogni $M \leq N$. Poiché H è un gruppo profinito per la Proposizione 2.8 si ha che $\bigcap\{M \text{ con } M \triangleleft_O H\} = 1_H$. Dunque per la Proposizione 4.2 punto 3 si ha che H è isomorfo come gruppo topologico a $s\varprojlim H/M =: \hat{H}$. Per definizione di limite inverso esiste ed è unico un omomorfismo continuo χ tale che il seguente diagramma sia commutativo



dove p_M è la mappa proiezione.
Consideriamo la seguente mappa

$$\begin{array}{rccc} \delta: & H & \longrightarrow & \hat{H} \\ & h & \longmapsto & (hM)_{M \triangleleft_O H} \end{array}$$

che abbiamo già visto essere un isomorfismo fra gruppi topologici. Chiaramente risulta che $p_M \circ \delta = q_M$. Se consideriamo la mappa $\hat{\theta} = \delta^{-1} \circ \chi$ si ha che $q_M \circ \hat{\theta} = \hat{\theta}_M$.



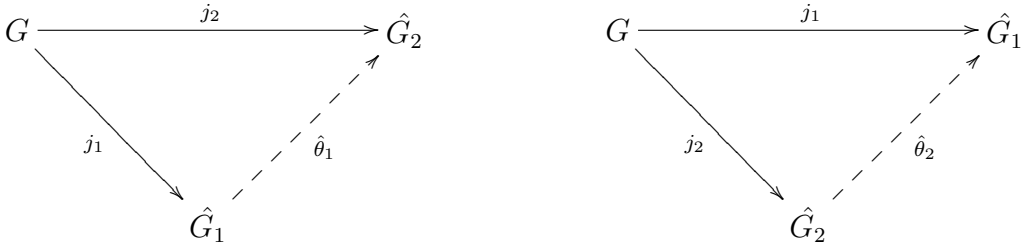
Infatti $(p_M \circ \delta) \circ (\delta^{-1} \circ \chi) = p_M \circ \chi = \hat{\theta}_M$. Quindi la mappa $\hat{\theta}$ fa commutare la parte destra del diagramma iniziale. Proviamo che la mappa $\hat{\theta}$ rende commutativa la parte sinistra

del diagramma, cioè $\hat{\theta} \circ j = \theta$, concludendo così la dimostrazione. Poiché per ogni $M \triangleleft_O H$ abbiamo visto che $\hat{\theta}_M = q_M \circ \hat{\theta}$ e $\hat{\theta}_M \circ j = q_M \circ \theta$ allora $q_M \circ (\hat{\theta} \circ j) = q_M \circ \theta$. Quindi per ogni $M \triangleleft_O H$ e per ogni $g \in G$ si ha che $q_M((\hat{\theta} \circ j)(g)) = q_M(\theta(g))$ e poiché q_M è un omomorfismo di gruppi si ha che $q_M((\hat{\theta} \circ j)(g) \cdot \theta(g)^{-1}) = 1_{H/M}$. Dunque $(\hat{\theta} \circ j)(g) \cdot \theta(g)^{-1} \in \ker q_M$ per ogni $g \in G$ e per ogni $M \triangleleft_O H$. Allora $(\hat{\theta} \circ j)(g) \cdot \theta(g)^{-1} \in \bigcap\{M \text{ con } M \triangleleft_O H\}$ per ogni G. Ma $\bigcap\{M \text{ con } M \triangleleft_O H\} = 1_G$ essendo H un gruppo profinito, quindi $\hat{\theta} \circ j = \theta$.
Vediamo ora l'unicità. Sia $\tau : \hat{G} \longrightarrow H$ tale che $\tau \circ j = \theta = \hat{\theta} \circ j$, allora per ogni $M \triangleleft_O H$ si ha che $q_M \circ \tau \circ j = q_M \circ \theta = q_M \circ \hat{\theta} \circ j$. Per ipotesi esiste ed è unica la mappa $\hat{\theta}_M$ tale che $\hat{\theta}_M \circ j = q_M \circ \theta$. Quindi $q_M \circ \tau = \hat{\theta}_M = q_M \circ \hat{\theta}$ per ogni $M \triangleleft_O H$, allora per ogni $\hat{g} \in \hat{G}$ si ha che $q_M(\tau(\hat{g}) \cdot \hat{\theta}(\hat{g})^{-1}) = 1_{H/M}$. Quindi per ogni $\hat{g} \in \hat{G}$ per ogni $M \triangleleft_O H$ si ha che $\tau(\hat{g}) \cdot \hat{\theta}(\hat{g})^{-1} \in \ker q_M = M$. Dunque per ogni $\hat{g} \in \hat{G}$ si ha che $\tau(\hat{g}) = \hat{\theta}(\hat{g})$.

□

Teorema 5.4. *Siano G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Se $(\hat{G}_1, j_1)$ e $(\hat{G}_2, j_2)$ sono due completamenti di G rispetto a I allora esiste un isomorfismo $\alpha : \hat{G}_1 \longrightarrow \hat{G}_2$ tale che $\alpha \circ j_1 = j_2$.*

Dimostrazione. Per ipotesi j_1 e j_2 sono due omomorfismi continui. Allora esiste ed è unico l'omomorfismo continuo $\hat{\theta}_1$ tale che $\hat{\theta}_1 \circ j_1 = j_2$ ed esiste ed è unico l'omomorfismo continuo $\hat{\theta}_2$ tale che $\hat{\theta}_2 \circ j_2 = j_1$.



Quindi $\hat{\theta}_1 \circ \hat{\theta}_2 \circ j_2 = j_2$ e $\hat{\theta}_2 \circ \hat{\theta}_1 \circ j_1 = j_1$. Ma $id_{\hat{G}_1} \circ j_1 = j_1$ e $id_{\hat{G}_2} \circ j_2 = j_2$. Dunque per l'unicità delle mappe $\hat{\theta}_1$ e $\hat{\theta}_2$ si ha che $\hat{\theta}_1 : \hat{G}_1 \longrightarrow \hat{G}_2$ è un isomorfismo di gruppi topologici e vale che $\hat{\theta}_1 \circ j_1 = j_2$.

□

Proposizione 5.5. *Siano G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Se $(\hat{G}, j)$ è un completamento di G rispetto a I allora $j(G)$ è denso in $\hat{G}$ e $\ker j = \bigcap_{K \in I} K$.*

Dimostrazione. Dimostriamo prima l'enunciato per un particolare completamento. Nella Proposizione 5.2 abbiamo dimostrato che $\hat{G} := s\lim_{\longleftarrow K \in I} G/K$ e $j : G \longrightarrow \hat{G}$ con $j(g) = (gK)_{K \in I}$ formano un completamento di G. Abbiamo già dimostrato nella Proposizione 4.2 punto 2 che $j(G)$ è denso in $\hat{G}$ e che $\ker j = \bigcap_{K \in I} K$.

Se $(\hat{G}_1, j_1)$ è un altro completamento di G rispetto a I allora esiste un isomorfismo di spazi topologici $\alpha : \hat{G} \longrightarrow \hat{G}_1$ tale che $\alpha \circ j = j_1$. Dimostriamo che $j_1(G)$ è denso in $\hat{G}_1$. Chiaramente $\overline{(\alpha \circ j)(G)} \subseteq \hat{G}_1$. Mostriamo che vale anche che $\hat{G}_1 \subseteq \overline{(\alpha \circ \theta)(G)}$. Sia $g_1 \in \hat{G}_1$ se per assurdo esiste un intorno U_{g_1} di g_1 in $\hat{G}_1$ tale che $U_{g_1} \cap (\alpha \circ \theta)(G) = \emptyset$ allora $\alpha^{-1}(U_{g_1}) \cap \theta(G) = \emptyset$, ma $\alpha^{-1}(U_{g_1})$ è un intorno di $\alpha^{-1}(g) \in \hat{G}$ che è assurdo.
Vale che $\ker j_1 = \ker j$, infatti per ogni $g \in G$ si ha che $j_1(g) = \alpha(j(g)) = 1$ se e solo se $j(g) = 1$ poiché α è un omomorfismo iniettivo. Dunque $\ker j_1 = \ker j = \bigcap_{K \in I} K$.

□

$(\hat{G}, j)$ è detto completamento di G proprio per il fatto che $j(G)$ è denso in $\hat{G}$.
Se p è un primo il completamento pro-p di G è il completamento di G rispetto alla famiglia I di tutti i sottogruppi normali di indice una potenza di p. Si noti che tale I è effettivamente una base filtro infatti se H_1 e H_2 sono due sottogruppi di G con indice una potenza di p allora anche $H_1 \cap H_2$ è un sottogruppo di G di indice una potenza di p. Per la Proposizione 5.2 si ha che il completamento di G è un pro-p gruppo ovvero il limite inverso di un sistema inverso di p-gruppi finiti.

Osservazione 5.6. *Sia G un gruppo ed I una base filtro non vuota di sottogruppi normali di G di indice finito. Sia $(\hat{G}, j)$ un completamento di G rispetto a I. Se G^* è un gruppo topologico e $f : \hat{G} \longrightarrow G^*$ è un isomorfismo di gruppi topologici allora $(G^*, f \circ j)$ è un completamento di G rispetto a I.*

Dimostrazione. Si ha che G^* è un gruppo profinito poiché è quasi compatto e totalmente disconnesso essendo omeomorfo a $\hat{G}$. Siano H un gruppo finito e $\theta : G \longrightarrow H$ un omomorfismo continuo. Vogliamo provare che esiste ed è unico θ^* omomorfismo continuo tale che $\theta^* \circ (f \circ j) = \theta$. Per ipotesi esiste ed è unico un omomorfismo continuo $\hat{\theta}$ tale che $\hat{\theta} \circ j = \theta$. Sia $\theta^* := \hat{\theta} \circ f^{-1}$. Si ha che θ^* è un omomorfismo continuo e $\theta^* \circ (f \circ j) = \hat{\theta} \circ j = \theta$. Se $\tilde{\theta}$ è un altro omomorfismo continuo tale che $\tilde{\theta} \circ (f \circ j) = \theta$ allora $(\tilde{\theta} \circ f) \circ j = \hat{\theta} \circ j$ dunque per l'unicità della mappa $\hat{\theta}$ si ha che $\hat{\theta} = \tilde{\theta} \circ f$ e quindi $\tilde{\theta} = \theta^*$.

□

Pro-p completamento di $\mathbb{Z}$

Osservazione 5.7. *Siano M e G due insiemi. Sia $f : G \longrightarrow M$ una biezione.*

1. *Se $(M, +)$ è un gruppo allora anche G è un gruppo con la seguente operazione: $g_1 +_G g_2 := f^{-1}(f(g_1) +_M f(g_2))$ per ogni $(g_1, g_2) \in G \times G$. Inoltre se $(M, +)$ è abeliano anche $(G, +_G)$ è abeliano.*

2. *Se $(M, +)$ è un gruppo allora con l'operazione $+_G$ su G la mappa f diventa un isomorfismo di gruppi.*

3. *Se* $(M,+,\cdot)$ *è un anello allora* $(G,+_G)$ *è un anello con la seguente operazione* $g_1 \cdot_G g_2 := f^{-1}(f(g_1)\cdot_M f(g_2))$ *per ogni* $(g_1,g_2)\in G\times G$.

4. *Se* $(M,+,\cdot)$ *è un anello allora con le operazioni* $+_G$, $\cdot_G$ *su* G *la mappa* f *diventa un isomorfismo di anelli.*

5. *Se* (M,τ) *è uno spazio topologico allora anche* (G,γ) *è uno spazio topologico dove* $A\in\gamma$ *se e solo se* $f(A)\in\tau$.

6. *Se* (M,τ) *è uno spazio topologico se in* G *consideriamo la topologia* γ *allora* f *è un omeomorfismo.*

7. *Se* $(M,+,\tau)$ *è un gruppo topologico allora anche* $(G,+_G,\gamma)$ *è un gruppo topologico.*

Dimostrazione. La dimostrazione dei punti 1, 2, 3 e 4 sono delle semplici verifiche. Proviamo ad esempio per il punto 3 che per ogni $g_1,g_2,g_3\in G$ si ha che $g_1\cdot_G(g_2+_G g_3) = = g_1\cdot_G g_2 +_G g_1\cdot_G g_3$. Si ha che

$$g_1\cdot_G(g_2+_G g_3) = f^{-1}(f(g_1)\cdot f(g_2+_G g_3)) = f^{-1}\left(f(g_1)\cdot f\left(f^{-1}(f(g_2)+f(g_3))\right)\right)$$

che essendo M un anello risulta essere uguale a

$$f^{-1}(f(g_1)\cdot f(g_2)+f(g_1)\cdot f(g_3)) = f^{-1}(f(g_1\cdot_G g_2)+f(g_1\cdot_G g_3)) = g_1\cdot_G g_2 +_G g_1\cdot_G g_3.$$

Anche i punti 5, 6 e 7 sono delle semplici verifiche. Ad esempio dimostriamo per il punto 7 che la mappa

$$\begin{array}{rccc}\chi: & G\times G & \longrightarrow & G\\ & (g_1,g_2) & \longmapsto & g_1+_G g_2\end{array}$$

è continua. Basta osservare che la mappa

$$\begin{array}{rccc}\varphi: & G\times G & \longrightarrow & M\times M\\ & (g_1,g_2) & \longmapsto & (f(g_1),f(g_2))\end{array}$$

è continua e che $\chi = f^{-1}\circ\chi'\circ\varphi$ dove χ' è la mappa che ad ogni $m_1,m_2\in M\times M$ asocia m_1+m_2 in M.

□

Consideriamo l'insieme $\mathbb{Z}_p$ delle somme formali infinite $\displaystyle\sum_{j=0}^{\infty} a_j p^j$ con $0\le a_j<p$ per ogni j. Sia

$$\begin{array}{rccc}\theta: & \mathbb{Z}_p & \longrightarrow & s\varprojlim \mathbb{Z}/\mathbb{Z}p^i\\ & \displaystyle\sum_{j=0}^{\infty} a_j p_j & \longmapsto & ([a_0+a_1p+\ldots+a_{i-1}p^{i-1}]_{p^i})_{i=1,2,\ldots}.\end{array}$$

Mostriamo che θ è una applicazione biunivoca.
Per ogni $i \leq j$ siano

$$\begin{array}{rccc} \varphi_{ij}: & \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ & [k]_{p^j} & \longmapsto & [k]_{p^i} \end{array}$$

le mappe del sistema inverso.
Per ogni $\sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p$ si ha che $\theta(\sum_{j=0}^{\infty} a_j p^j) \in s\varprojlim \mathbb{Z}/\mathbb{Z}p^i$ infatti per ogni $i \leq j$ si ha

$$\varphi_{ij}([a_0 + a_1 p + \ldots + a_{j-1}p^{j-1}]_{p^j}) = [a_0 + a_1 p + \ldots + a_{j-1}p^{j-1}]_{p^i}.$$

Inoltre θ è ben definita poiché $\sum_{j=0}^{\infty} a_j p^j = \sum_{j=0}^{\infty} b_j p^j$ se e solo se $a_j = b_j$ per ogni j.
Mostriamo che θ è iniettiva. Se $\theta(\sum_{j=0}^{\infty} a_j p^j) = \theta(\sum_{j=0}^{\infty} b_j p^j)$ allora per ogni $i = 1, 2, \ldots$ si ha che $[a_0 + a_1 p + \ldots + a_{i-1}p^{i-1}]_{p^i} = [b_0 + b_1 p + \ldots + b_{i-1}p^{i-1}]_{p^i}$. Esiste $S_1 \in \mathbb{Z}$ tale che $a_0 = b_0 + S_1 p$ quindi essendo $0 \leq a_0 < p$ e $b_0 < p$ si ha che $S_1 = 0$, dunque $a_0 = b_0$. Supponiamo per ipotesi induttiva che $a_j = b_j$ per ogni $j < k$ e proviamo che $a_k = b_k$. Per ipotesi $[a_0 + a_1 p + \ldots + a_k p^k]_{p^{k+1}} = [a_0 + a_1 p + \ldots + a_k p^k]_{p^{k+1}}$ quindi esiste $S_{k+1} \in \mathbb{Z}$ tale che $a_k p^k = b_k p^k + S_{k+1} p^{k+1}$, ma $0 \leq a_k < p$ e $b_k < p$ quindi $a_k = b_k$. Per ogni $j = 0, 1, \ldots$ si ha che $a_j = b_j$.
Mostriamo che θ è suriettiva. Sia $z = ([a_i]_{p^i})_{i=1,2\ldots} \in s\varprojlim \mathbb{Z}/\mathbb{Z}p^i$ con $0 \leq a_i < p^i$ per ogni i. Poiché $[a_1]_p = [a_2]_p$ esiste $S_1 \in \mathbb{Z}$ tale che $a_2 = a_1 + S_1 p$. Necessariamente $0 \leq S_1 < p$. Supponiamo per ipotesi induttiva che esistono S_j per $j = 1, 2, \ldots, k$ maggiori o uguali a zero e minori di p tali che per ogni $j < k$ si ha $a_{j+1} = a_1 + S_1 p + \ldots + S_j p^j$. Poiché $[a_k]_{p^k} = [a_{k+1}]_{p^k}$ allora esiste $S_{k+1} \in \mathbb{Z}$ maggiore o uguale a zero e minore di p tale che $a_{k+1} = a_k + S_k p^k$, ma $a_k = a_1 + S_1 p + \ldots + S_{k-1} p^{k-1}$ e quindi $a_{k+1} = a_1 + S_1 p + \ldots + S_k p^k$. Quindi per ogni k esistono $S_j \in \mathbb{Z}$ maggiori o uguali a zero e minori di p per $j = 1, 2 \ldots$ tali che $a_{k+1} = a_1 + S_1 p + \ldots + S_k p^k$. Poniamo $S_0 := a_1$. Sia $w = \sum_{j=0}^{\infty} S_j p^j \in \mathbb{Z}_p$. Si ha che $\theta(w) = ([S_0 + S_1 p + \ldots + S_{i-1}p^{i-1}]_{p^i})_{i=1,2\ldots} = z$.

Tramite θ definiamo la somma in $\mathbb{Z}_p$.

$$\sum a_j p^j + \sum b_j p^j := \theta^{-1}(\theta(\sum a_j p^j) + \theta(\sum b_j p^j)) =$$

$$= \theta^{-1}\left(\left([(a_0 + b_0) + (a_1 + b_1)p + \ldots + (a_{i-1} + b_{i-1})p^{i-1}]_{p^i}\right)_{i=1,2,\ldots}\right).$$

Tramite θ definiamo il prodotto in $\mathbb{Z}_p$.

$$\sum a_j p^j \cdot \sum b_j p^j := \theta^{-1}(\theta(\sum a_j p^j) \cdot \theta(\sum b_j p^j)) =$$

$$= \theta^{-1}\left(\left([a_0b_0]_{p^i} + [(a_0b_1 + a_1b_0)p]_{p^i} + \ldots + [(a_0b_i + a_1b_{i-1} + \ldots + a_ib_0)p^{i-1}]_{p^i}\right)_{i=1,2,\ldots}\right).$$

Con tali operazioni $\mathbb{Z}_p$ è un anello. Tramite la biezione θ si può rendere $\mathbb{Z}_p$ un gruppo topologico come precedentemente mostrato. La mappa θ risulta quindi un omomorfismo di gruppi topologici.
Si noti che poiché $\mathbb{Z}_p$ è isomorfo come gruppo topologico a $s\varprojlim \mathbb{Z}/\mathbb{Z}p^i$ si ha che $(\mathbb{Z}_p, \varphi_i^*)$ è un limite inverso di $(\mathbb{Z}/\mathbb{Z}p^i, \varphi_{ij})$, dove $\varphi_i^* := p_i \circ \theta$ con p_i proiezioni.

Mostriamo che per ogni z intero maggiore o uguale a zero esistono $m \in \mathbb{N}$ e $a_0, \ldots, a_m$ interi tali che $z = a_0 + a_1p + \ldots + a_mp^m$ con $0 \leq a_j < p$ per ogni j.
Sia a_0 l'unico intero maggiore o uguale a zero e minore di p tale che $[z]_p = [a_0]_p$. Poiché $p|(z - a_0)$ possiamo considerare $z_1 := \frac{z-a_0}{p}$. Sia a_1 l'unico intero maggiore o uguale a zero e minore di p tale che $[z_1]_p = [a_1]_p$. In generale poiché $p|(z_{m-1} - a_{m-1})$ possiamo considerare $z_m := \frac{z_{m-1}-a_{m-1}}{p}$ e definire a_m come l'unico intero maggiore o uguale a zero e minore di p tale che $[z_m]_p = [a_m]_p$. Supponiamo che per un certo intero m abbiamo che $z_m < p$ e in tale caso poniamo $a_m = z_m$. Poiché $z_m = \frac{z_{m-1}-a_{m-1}}{p}$ abbiamo che $z_{m-1} = a_{m-1} + z_mp$. Ma $z_{m-1} = \frac{z_{m-2}-a_{m-2}}{p}$ dunque $z_{m-2} = a_{m-2} + a_{m-1}p + a_mp^2$. Si ha allora che $z_1 = z_{m-(m-1)} = a_1 + a_2p + \ldots + a_mp^{m-1}$ quindi $z = a_0 + a_1p + \ldots + a_mp^m$.
Consideriamo la mappa $i : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ definita nel modo seguente.
Se z è un intero maggiore o uguale a zero, $z = a_0 + a_1p + \ldots + a_mp^m$ dove gli a_j sono interi $0 \leq a_j < p$, allora $i(z) = a_0 + a_1p + \ldots + a_mp^m$. Se $k = -z$ con z un intero maggiore di zero, $z = a_0 + a_1p + \ldots + a_mp^m$ dove gli a_j sono interi $0 \leq a_j < p$, allora $i(k) = -(a_0 + a_1p + \ldots + a_mp^m)$. La mappa i è continua poiché in $\mathbb{Z}$ consideriamo la topologia discreta.
Sia $I := \{\mathbb{Z}p^i \text{ con } i = 1, 2, \ldots\}$. Si ha che I è una base filtro di sottogruppi di $\mathbb{Z}$ con indice finito. Un completamento di $\mathbb{Z}$ rispetto a I per la Proposizione 5.2 è $(s\varprojlim \mathbb{Z}/\mathbb{Z}p^i, j)$ dove j è la seguente mappa.

$$\begin{array}{rccc} j: & \mathbb{Z} & \longrightarrow & s\varprojlim \mathbb{Z}/\mathbb{Z}p^i \\ & k & \longmapsto & ([k]_{p^i})_{i=1,2\ldots} \end{array}$$

Mostriamo che $j = \theta \circ i$. Ad esempio se z è un intero positivo, $z = a_0 + a_1p + \ldots + a_mp^m$, poiché j è un omomorfismo di gruppi si ha che $j(-z) = -([z]_{p^i})_i$ che è uguale a $-([a_0 + a_1p + \ldots + a_mp^m]_{p^i})_i$. Mentre $\theta \circ i(-z) = \theta(-(a_0 + a_1p + \ldots + a_mp^m)) = = -([a_0 + a_1p + \ldots + a_mp^m]_{p^i})_i$.
Poiché $\theta^{-1} : s\varprojlim \mathbb{Z}/\mathbb{Z}p^i \longrightarrow \mathbb{Z}_p$ è un omomorfismo di gruppi topologici per l'Osservazione 5.6 si ha che $(\mathbb{Z}_p, i)$ è un completamento di $\mathbb{Z}$ rispetto a I.
Si noti che poiché la mappa j è iniettiva si ha che i è un omomorfismo di gruppi iniettivo.

Lemma 5.8. *Sia G un gruppo. Siano H e K due sottogruppi di G tali che $K \subseteq H$. Allora $|G : K| = |G : H||H : K|$.*

Dimostrazione. Esistono $g_1, \ldots, g_n \in G$, con $g_1H, \ldots, g_nH$ distinti fra loro, tali che $G = \bigcup_{i=i}^{n} g_iH$. Esistono $h_1, \ldots, h_m \in H$, con $h_1K, \ldots, h_mK$ distinti fra loro tali che $H = \bigcup_{j=i}^{m} h_jK$. Allora $H = \bigcup_{i=1}^{n} g_i(\bigcup_{j=1}^{m} h_jK) = \bigcup_{i=1}^{n}\bigcup_{j=1}^{m} g_ih_jK$. Se esistono $i, s \in \{1, \ldots, n\}$ e $j, r \in \{1, \ldots, m\}$ tali che $g_i(h_jK) = g_s(h_rK)$, poiché $K \subseteq H$, allora $g_iH = g_sH$. Dunque $g_i = g_s$. Allora $h_jK = h_rK$, quindi $h_j = h_r$.

□

Lemma 5.9. *Sia G un gruppo. Siano H e K due sottogruppi di G tali che $K \subseteq H$. Se l'indice di K in G è uguale all'indice di H in G allora $K = H$.*

Dimostrazione. Per il Lemma 5.8 si ha che $|H : K| = 1$ quindi $H = K$.

□

Proposizione 5.10. *H è un sottogruppo aperto di $\mathbb{Z}_p$ se e solo se esiste $i \in \mathbb{N} \cup \{0\}$ tale che $H = p^i\mathbb{Z}_p$.*

Dimostrazione. Mostriamo per induzione che

$$p^i\mathbb{Z}_p = \{\sum_{j=i}^{\infty} a_jp^j \text{ con } a_j \text{ interi, } 0 \leq a_j < p\}$$

per ogni i. Si ha che

$$p \cdot \sum_{j=0}^{\infty} a_jp^j = \theta^{-1}\left(\left([p]_{p^i} \cdot [a_0 + a_1p \ldots + a_{i-1}p^{i-1}]_{p^i}\right)_{i=1,2\ldots}\right) =$$

$$= \theta^{-1}\left(\left([a_0p + a_1p^2 + \ldots + a_{i-2}p^{i-1} + a_{i-1}p^i]_{p^i}\right)_{i=1,2\ldots}\right) = \sum_{j=1}^{\infty} a_{j-1}p^j.$$

Se supponiamo che $p^k(\sum_{j=0}^{\infty} a_jp^j) = \sum_{j=k}^{\infty} a_{j-k}p^j$ per ogni $k < s$ allora poiché $\mathbb{Z}_p$ è un anello si ha che $p^s(\sum_{j=0}^{\infty} a_jp^j) = p(\sum_{j=s-1}^{\infty} a_{j-(s-1)}p^j) = \sum_{j=s}^{\infty} a_{j-s}p^j$.
Mostriamo che per ogni i vale che $p^i\mathbb{Z}_p$ è un sottogruppo aperto di $\mathbb{Z}_p$ di indice p^i. Consideriamo la mappa

$$\begin{array}{rccc} \varphi_i^* : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/\mathbb{Z}p^i \\ & \sum_{j=0}^{\infty} a_jp^j & \longmapsto & [a_0 + a_1p + \ldots + a_{i-1}p^{i-1}]_{p^i}. \end{array}$$

Proviamo che $\ker \varphi_i^* = \{\sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p \text{ tali che } [a_0 + \ldots + a_{i-1}p^{i-1}]_{p^i} = [0]_{p^i}\} = p^i\mathbb{Z}_p$. Se ciò è vero allora $p^i\mathbb{Z}_p = \varphi_i^{*-1}([0]_{p^i})$ è un sottogruppo aperto di $\mathbb{Z}_p$. Se $\sum_{j=0}^{\infty} a_j p^j \in \ker \varphi_i^*$ allora esiste $S \in \mathbb{Z}$ tale che $a_0 + \ldots + a_{i-1}p^{i-1} = Sp^i$, quindi $p|a_0$. Necessariamente allora $a_0 = 0$. Allora $p|a_1$ e quindi $a_1 = 0$. Analogamente $p|a_j$ per ogni $j = 3, \ldots, i-1$ e quindi $a_j = 0$ per ogni j. Dunque $z = \sum_{j=i}^{\infty} a_j p^j \in p^i\mathbb{Z}_p$. Chiaramente $p^i\mathbb{Z}_p \subseteq \ker \varphi_i^*$.
Sia H un sottogruppo aperto di $\mathbb{Z}_p$. Poiché $s\varprojlim \mathbb{Z}/\mathbb{Z}p^i$ è abeliano anche $\mathbb{Z}_p$ è abeliano, quindi ogni sottogruppo di $\mathbb{Z}_p$ è normale.
Sia $\mathcal{C} := \{\text{Gruppi di ordine una potenza di } p\}$ che è chiuso per quozienti. Abbiamo già osservato che $\mathbb{Z}_p$ è un pro-$\mathcal{C}$ gruppo, quindi se $H \triangleleft_O \mathbb{Z}_p$ allora per il Teorema 4.4 punto 4' si ha che $\mathbb{Z}_p/H \in \mathcal{C}$ dunque l'indice di H è una potenza di p. Sia $|\mathbb{Z}_p/H| = p^r$. Se $zH \in \mathbb{Z}_p/H$ allora $p^r \cdot zH = zH + \ldots + zH$ (p^r volte)$= (p^r z)H$ e $p^r zH = 0H$. Dunque $p^r\mathbb{Z}_p \subseteq H$.
Poiché φ_r^* è un omomorfismo di gruppi suriettivo si ha che $\mathbb{Z}_p/\ker \varphi_r^* = \mathbb{Z}_p/p^r\mathbb{Z}_p$ è isomorfo come gruppo a $\mathbb{Z}/\mathbb{Z}p^r$ quindi $|\mathbb{Z}_p/p^r\mathbb{Z}_p| = p^r$.
Dunque $p^r\mathbb{Z}_p \subseteq H$ e $p^r\mathbb{Z}_p$ ha indice in $\mathbb{Z}_p$ uguale all'indice di H in $\mathbb{Z}_p$ quindi per il Lemma 5.9 si ha $p^r\mathbb{Z}_p = H$.

□

Corollario 5.11. *C è un sottogruppo chiuso in $\mathbb{Z}_p$ se e solo se $C = \{0\}$ oppure esiste $i \in \mathbb{N} \cup \{0\}$ tale che $C = p^i\mathbb{Z}_p$.*

Dimostrazione. Come già abbiamo visto per i diverso da 0 si ha che $p^i\mathbb{Z}_p = \varphi_i^{*-1}([0]_{p^i})$ e quindi per i diverso da 0 si ha che $p^i\mathbb{Z}_p$ è un chiuso. Poiché $\mathbb{Z}_p$ è un gruppo profinito in particolare è di Hausdorff quindi $\{0\}$ è un chiuso.
Poiché $\mathbb{Z}_p$ è un gruppo profinito allora $\mathbb{Z}_p$ è quasi compatto e totalmente disconnesso, quindi dalla Proposizione 2.8 punto c) 2 segue che per ogni chiuso C in $\mathbb{Z}_p$ vale che $C = \bigcap\{NC \text{ con } N \triangleleft_O \mathbb{Z}_p\}$. Poiché NC è un aperto di $\mathbb{Z}_p$, esiste $r \in \mathbb{N} \cup \{0\}$ tale che $NC = p^r\mathbb{Z}_p$. Quindi C è intersezione di insiemi della forma $p^i\mathbb{Z}_p$. Poiché per ogni i si ha che $p^i\mathbb{Z}_p \supseteq p^{i+1}\mathbb{Z}_p$ per il principio del minimo esiste $k \in \mathbb{N}$ tale che $C = p^k\mathbb{Z}_p$.

□

Esempio 8. *Per ogni primo p esistono dei sottogruppi di $\mathbb{Z}_p$ che non sono né aperti né chiusi di $\mathbb{Z}_p$.*

Dimostrazione. Consideriamo $i(\mathbb{Z}) \subseteq \mathbb{Z}_p$. Poiché i è un omomorfismo di gruppi allora $i(\mathbb{Z})$ è un sottogruppo di $\mathbb{Z}_p$. Poiché $(\mathbb{Z}_p, i)$ è un completamento pro-p di $\mathbb{Z}$ si ha che $\overline{i(\mathbb{Z})} = \mathbb{Z}_p$. Se $i(\mathbb{Z})$ fosse un chiuso di $\mathbb{Z}_p$ allora $i(\mathbb{Z})$ sarebbe uguale a $\mathbb{Z}_p$. Proviamo che

esiste un elemento di $\mathbb{Z}_p$ che non appartiene a $i(\mathbb{Z})$ per ogni primo p. Si può facilmente verificare per induzione che per ogni primo p e per ogni $n \in \mathbb{N} \cup \{0\}$ si ha che $\sum_{j=0}^{n} p^j < p^{n+1}$.

Sia $x = \sum_{j=0}^{\infty} a_j p^j$ con $a_j = 1$ se j è pari $a_j = 0$ se j è dispari. Chiaramente $x \in \mathbb{Z}_p$ per ogni p. Supponiamo per assurdo che esista un intero k tale che $i(k) = x$. Possiamo supporre che $-p^s \leq k \leq p^s$ per un certo $s \in \mathbb{N}$. Si avrebbe che $(\theta^{-1} \circ j)(k) = x$, quindi $j(k) = \theta(x)$. Allora

$$([k]_{p^i})_{i=1,2,\ldots} = ([\sum_{j=0}^{i-1} a_j p^j]_{p^i})_{i=1,2,\ldots}.$$

In particolare esiste un intero T_s tale che $k = \sum_{j=0}^{s-1} a_j p^j + T_s p^s$. Chiaramente $T_s \leq 0$. Poiché $\sum_{j=0}^{s-1} a_j p^j \leq \sum_{j=0}^{s-1} p^j < p^s$ allora $k = \sum_{j=0}^{s-1} a_j p^j + T_s p^s < (1 + T_s) p^s$ che è minore o uguale di $-p^s$ se $T_s \leq -2$. Quindi $T_s \in \{-1, 0\}$. Sia s pari. Si avrebbe che

$$[k]_{p^{s+1}} = [\sum_{j=0}^{s-1} a_j p^j + T_s p^s]_{p^{s+1}} = [\sum_{j=0}^{s-1} a_j p^j + 1 \cdot p^s]_{p^{s+1}}.$$

Allora $[T_s p^s]_{p^{s+1}} = [p^s]_{p^{s+1}}$ che risulta essere assurdo se $T_s = 0$. Se $T_s = -1$ risulta essere assurdo se p è dispari. Nel caso in cui p è pari si ha però che $[\sum_{j=0}^{s-1} a_j p^j - 2^s]_{2^{s+2}} =$
$= [\sum_{j=0}^{s-1} a_j p^j + 1 \cdot 2^s + 0 \cdot 2^{s+1}]_{2^{s+2}}$ quindi $[0]_{2^{s+2}} = [2^{s+1}]_{2^{s+2}}$, che è assurdo.

Sia s dispari. Si avrebbe che $[\sum_{j=0}^{s-1} a_j p^j + T_s p^s]_{p^{s+1}} = [\sum_{j=0}^{s-1} a_j p^j + 0 p^s]_{p^{s+1}}$. Dunque $T_s \neq -1$. Inoltre si avrebbe che $[\sum_{j=0}^{s-1} a_j p^j + 0]_{p^{s+2}} = [\sum_{j=0}^{s-1} a_j p^j + 0 p^s + 1 p^{s+1}]_{p^{s+2}}$. Quindi $[p^{s+1}]_{p^{s+2}} =$
$= [0]_{p^{s+2}}$ che è assurdo.
Poiché $\mathbb{Z}_p$ è un gruppo topologico per l'Osservazione 2.2 punto c) si ha che $i(\mathbb{Z})$ non può essere un aperto di $\mathbb{Z}_p$.

□

Proposizione 5.12. *$\mathbb{Z}_p$ è un dominio di integrità.*

Dimostrazione. Sia $x \in \mathbb{Z}_p \setminus \{0\}$. Si dimostra facilmente che

$$\begin{array}{rccc} \psi_x : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & u & \longmapsto & ux \end{array}$$

è un omomorfismo di gruppi continuo.
Sia $U_x := \psi_x^{-1}(0) = \{u \in \mathbb{Z}_p \text{ tali che } ux = 0\}$. Poiche 0 è chiuso in $\mathbb{Z}_p$ allora U_x è un sottogruppo chiuso di $\mathbb{Z}_p$. Allora U_x è uguale a 0 oppure esiste $r \in \mathbb{N}$ tale che $U_x = p^r\mathbb{Z}_p$. Supponiamo per assurdo che esista un r tale che per ogni $z \in \mathbb{Z}_p$ si abbia $p^r z \in U_x$ cioè per ogni $z \in \mathbb{Z}_p$ si abbia che $p^r zx = 0$. Sia $x = \sum_{j=0}^{\infty} b_j p^j$, poiché $x \neq 0$ esiste $s \in \mathbb{N}$ tale che $b_s \neq 0$. Sia $z := 1_{\mathbb{Z}_p}$, allora $p^r zx = p^r x = \sum_{j=r}^{\infty} b_{j-r} p^j$ che è diverso da 0. Necessariamente dunque $U_x = 0$, quindi $\mathbb{Z}_p$ è un dominio di integrità.

□

Proposizione 5.13. *$\mathcal{A}$ è un ideale di $\mathbb{Z}_p$ se e solo se $\mathcal{A}$ è un sottogruppo chiuso di $\mathbb{Z}_p$.*

Dimostrazione. Sia C un sottogruppo chiuso di $\mathbb{Z}_p$. Se $C = \{0\}$ allora C è un ideale, se $C = p^i\mathbb{Z}_p = \ker \varphi_i^*$ si ha che C è un ideale poiché $\varphi_i^* = p_i \circ \theta$ è un omomorfismo di anelli in quanto composizione di omomorfismi di anelli.
Sia $\mathcal{A}$ un ideale di $\mathbb{Z}_p$. Se $\mathcal{A} = \{0\}$ allora $\mathcal{A}$ è chiuso. Sia $\mathcal{A}$ diverso da $\{0\}$ e $x \in \mathcal{A} \setminus \{0\}$. Dato che $\mathcal{A}$ è un ideale di $\mathbb{Z}_p$ si ha che $x\mathbb{Z}_p \subseteq \mathcal{A}$.
Poiché

$$\begin{array}{rccc} \psi_x : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & u & \longmapsto & ux \end{array}$$

è continua e $\mathbb{Z}_p$ è quasi compatto allora anche $\psi_x(\mathbb{Z}_p) = x\mathbb{Z}_p$ è quasi compatto; ma $\mathbb{Z}_p$ è di Hausdorff quindi $x\mathbb{Z}_p \subseteq \mathbb{Z}_p$ è chiuso. Inoltre $x \cdot 1 = x \neq 0$ dunque esiste un intero r tale che $x\mathbb{Z}_p = p^r\mathbb{Z}_p$. Si ha quindi che $x\mathbb{Z}_p$ è aperto, allora $\mathcal{A}$ è un sottogruppo di $\mathbb{Z}_p$ contenente un insieme aperto non vuoto. Per l'Osservazione 2.2 punto d) si ha quindi che $\mathcal{A}$ è un sottogruppo aperto di $\mathbb{Z}_p$ dunque per l'Osservazione 2.2 punto c) si ha che $\mathcal{A}$ è un sottogruppo chiuso di $\mathbb{Z}_p$.

□

Corollario 5.14. *L'unico ideale massimale di $\mathbb{Z}_p$ è $p\mathbb{Z}_p$.*

Dimostrazione. Sia $\mathcal{A}$ un ideale di $\mathbb{Z}_p$. Se $\mathcal{A} = \{0\}$ allora $\mathcal{A}$ non è massimale poiché ad esempio $p\mathbb{Z}_p \supseteq \{0\}$. Poiché $p\mathbb{Z}_p \supseteq p^i\mathbb{Z}_p$ per ogni i allora $p\mathbb{Z}_p$ è un ideale massimale di $\mathbb{Z}_p$ e nessun altro ideale può essere massimale.

□

Proposizione 5.15. *Sia $x \in \mathbb{Z}_p$. Si ha che x è invertibile in $\mathbb{Z}_p$ se e solo se $x \notin p\mathbb{Z}_p$.*

Dimostrazione. Se $x = \sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p$ è invertibile in $\mathbb{Z}_p$ allora esiste $z = \sum_{j=0}^{\infty} b_j p^j \in \mathbb{Z}_p$ tale che $xz = 1_{\mathbb{Z}_p}$ quindi $\theta(x)\theta(z) = 1_{s\varprojlim \mathbb{Z}/\mathbb{Z}p^i} = ([1]_{p^j})_{j=1,2\ldots}$. In particolare vale che $[a_0 b_0]_p = [1]_p$, quindi $a_0 \neq 0$. Dunque $x \notin p\mathbb{Z}_p$.
Sia $x \notin p\mathbb{Z}_p$. Chiaramente $x\mathbb{Z}_p$ è un ideale di $\mathbb{Z}_p$. Ma $x\mathbb{Z}_p \nsubseteq p\mathbb{Z}_p$ poiché $x1_{\mathbb{Z}_p} = x \notin p\mathbb{Z}_p$. L'unico ideale di $\mathbb{Z}_p$ che non è contenuto in $p\mathbb{Z}_p$ è $\mathbb{Z}_p$ dunque $x\mathbb{Z}_p = \mathbb{Z}_p$. Allora esiste $z \in \mathbb{Z}_p$ tale che $xz = 1$ quindi x è invertibile in $\mathbb{Z}_p$.

□

Capitolo 6

Teoria di Galois

Definizione 6.1. Siano K e k due campi. K è una estensione di k e scriveremo $K \supseteq k$ se esiste un omomorfismo di anelli iniettivo da k in K.
Il grado dell'estensione $K \supseteq k$ verrà indicato con $[K : k]$. Per estensione finita si intenderà estensione di grado finito.

Definizione 6.2. Siano K e k due campi, con K estensione di k. Un elemento $\alpha \in K$ è algebrico su k se esiste un polinomio $g \in k[x]$ tale che $g(\alpha) = 0$.
L'estensione $K \supseteq k$ è algebrica se ogni elemento $\alpha \in K$ è algebrico su k.

Definizione 6.3. Sia k un campo e sia $p \in k[x]$ un polinomio non costante. Un campo di spezzamento di f su k è una estensione $K \supseteq k$ tale che

a) il polinomio p è prodotto di fattori lineari in $K[x]$;

b) se $\alpha_1, \ldots, \alpha_r$ sono le radici di p in K allora $K = k(\alpha_1, \ldots, \alpha_r)$.

Definizione 6.4. Siano K e k due campi. L'estensione di campi algebrica $K \supseteq k$ è detta normale se vale la seguente proprietà: se $g \in k[x]$ è un polinomio irriducibile con una radice in K allora g si fattorizza in fattori lineari in $K[x]$.

Definizione 6.5. Siano K e k due campi. Un polinomio $g \in k[x]$ è separabile se g non è costante e se le radici di g nel campo di spezzamento su k sono tutte semplici.
Siano $K \supseteq k$ una estensione algebrica e $\alpha \in K$. Se $p_\alpha \in k[x]$ è monico, ha come radice α e per ogni altro polinomio $g \in k[x]$ che ha α come radice si ha che $p_\alpha | g$ allora p_α è detto polinomio minimo di α su k.
Un elemento α di K è detto separabile se il suo polinomio minimo su k è separabile.
L'estensione algebrica $K \supseteq k$ è separabile se ogni elemento α di K è separabile.

Definizione 6.6. Siano K e k due campi. Una estensione algebrica $K \supseteq k$ è detta estensione di Galois se $K \supseteq k$ è normale e separabile.

Definizione 6.7. Siano K e k due campi. Sia $K \supseteq k$ una estensione algebrica di campi.

$$\mathrm{Gal}(K/k) := \{ \text{ automorfismi } \sigma : K \longrightarrow K \text{ tali che } \sigma(x) = x \text{ per ogni } x \in k\}.$$

Tale insieme risulta essere un gruppo ed è detto gruppo di Galois dell'estensione $K \supseteq k$.

Definizione 6.8. Se $F \supseteq k$ è una estensione di campi e H è un sottogruppo di $\mathrm{Gal}(F/k)$, il campo fisso di H è $F^H = \{\alpha \in F \text{ tali che } \sigma(\alpha) = \alpha \text{ per ogni } \sigma \in H\}$.
Si ha che F^H è un sottocampo di F contenente k.

Ricordiamo i seguenti risultati elementari della Teoria di Galois le cui dimostrazioni possone essere trovate nel libro *Galois Theory*, di David A.Cox [2].

Teorema 6.1 (Teorema della Torre)**.** *Siano $K \supseteq F$ e $F \supseteq k$ estensioni di campi. Si ha che $K \supseteq k$ è finita se e solo se $K \supseteq F$ e $F \supseteq k$ sono entrambe finite. In questo caso si ha $[K : k] = [K : F][F : k]$.*

Proposizione 6.2. *Sia $\gamma : K \longrightarrow L$ un isomorfismo di campi e $p \in K[x]$ un polinomio di grado maggiore di zero. Sia $\tilde{\gamma}$ la mappa così definita*

$$\begin{array}{rccc} \tilde{\gamma} : & K[x] & \longrightarrow & L[x] \\ & a_0 + a_1x + \ldots + a_nx^n & \longmapsto & \gamma(a_0) + \gamma(a_1)x + \ldots + \gamma(a_n)x^n. \end{array}$$

Siano E un campo di spezzamento di p su K e F un campo di spezzamento di $\tilde{\gamma}(p)$ su L. Allora esiste un isomorfismo di campi $\phi : E \longrightarrow F$ tale che $\phi_{|K} = \gamma$.

Proposizione 6.3. *Sia $F \supseteq k$ una estensione di campi. Si ha che F è il campo di spezzamento su k di un polinomio $p \in k[x]$ se e solo se $F \supseteq k$ è una estensione finita e normale.*

Proposizione 6.4. *Se $F \supseteq k$ è una estensione finita di campi e $\sigma \in \mathrm{Gal}(F/k)$ si ha*

1) *se $g \in k[x]$ è un polinomio non costante ed $\alpha \in F$ è una radice di g allora $\sigma(\alpha)$ è un'altra radice di g.*

2) *Se $F = k(\alpha_1, \ldots, \alpha_n)$ allora ogni $\sigma \in \mathrm{Gal}(F/k)$ è determinata dai valori che assume su $\alpha_1, \ldots, \alpha_n$.*

Proposizione 6.5. *Sia k un campo. Sia $f \in k[x]$ un polinomio non costante, $f = f_1 \cdot \ldots \cdot f_r$ con $f_1, \ldots, f_r \in k[x]$ irriducibili. Si ha che f è separabile se e solo se $f_1, \ldots, f_r$ sono separabili e a due a due non sono multipli l'uno dell'altro.*

Teorema 6.6 (Teorema dell'Elemento Primitivo)**.** *Sia $F \supseteq k$ una estensione finita, $F = k(\alpha_1, \ldots, \alpha_n)$, dove gli elementi $\alpha_1, \ldots, \alpha_n$ di F sono separabili su k. Allora esiste un elemento $\alpha \in F$ separabile su k, detto primitivo, tale che $F = k(\alpha)$.*

Teorema 6.7. *Siano F e k due campi tali che $F \supseteq k$ è una estensione finita. Si ha che F è il campo di spezzamento di un polinomio separabile di $k[x]$ se e solo se $F \supseteq k$ è di Galois.*

Teorema 6.8 (Teorema Fondamentale della Teoria di Galois classico)**.** *Sia $F \supseteq k$ una estensione di campi finita di Galois.*
Se M è tale che $F \supseteq M \supseteq k$ allora $F^{\mathrm{Gal}(F/M)} = M$. Inoltre $|\mathrm{Gal}(F/M)| = [F : M]$ e $[\mathrm{Gal}(F/k) : \mathrm{Gal}(F/M)] = [M : k]$.
Se H è un sottogruppo di $\mathrm{Gal}(F/k)$ si ha che $\mathrm{Gal}(F/F^H) = H$. Inoltre $[F : F^H] = |H|$ e $[F^H : k] = [\mathrm{Gal}(F/k) : H]$.
Allora la mappa

$$\begin{array}{rccc} \phi: & \{\textit{campi } M \textit{ tali che } F \supseteq M \supseteq k\} & \longrightarrow & \{\textit{sottogruppi } H \textit{ di } \mathrm{Gal}(F/k)\} \\ & M & \longmapsto & \mathrm{Gal}(F/M) \end{array}$$

è una biezione che rovescia le inclusioni la cui mappa inversa è

$$\begin{array}{rccc} \phi^{-1}: & \{\textit{sottogruppi } H \textit{ di } \mathrm{Gal}(F/k)\} & \longrightarrow & \{\textit{campi } M \textit{ tali che } F \supseteq M \supseteq k\} \\ & H & \longmapsto & F^H. \end{array}$$

Se inoltre un sottocampo M corrisponde ad un sottogruppo H tramite queste mappe, allora $M \supseteq k$ è di Galois se e solo se H è normale in $\mathrm{Gal}(F/k)$ e quando questo accade si ha che $\mathrm{Gal}(F/k)/H$ è isomorfo come gruppo a $\mathrm{Gal}(M/k)$.

Notazione. Per il resto del capitolo K e k saranno due campi tali che K è una estensione algebrica di k di Galois (non necessariamente finita).

Notazione. Siano K e k due campi. Sia $K \supseteq k$ una estensione di campi algebrica e di Galois. Poniamo

$$\mathcal{F} := \{F \text{ campo tale che } K \supseteq F \supseteq k \text{ e } F \supseteq k \text{ è finita e di Galois}\}$$

Definiamo una topologia in $\mathrm{Gal}(K/k)$.
Consideriamo l'insieme

$$\mathcal{B} := \{\sigma \circ \mathrm{Gal}(K/F) \text{ con } F \in \mathcal{F} \text{ e } \sigma \in \mathrm{Gal}(K/k)\}.$$

Se dimostriamo che $J := \{\mathrm{Gal}(K/F) \text{ con } F \in \mathcal{F}\}$ è una base filtro di sottogruppi normali di $\mathrm{Gal}(K/k)$ allora per l'Osservazione 5.1 si ha che $\mathrm{Gal}(K/k)$ è un gruppo topologico con la topologia che ha come base $\mathcal{B}$.
È chiaro che per ogni $F \in \mathcal{F}$ si ha che $\mathrm{Gal}(K/F)$ è un sottogruppo di $\mathrm{Gal}(K/k)$. Proviamo

che per ogni $F \in \mathcal{F}$ si ha che $\mathrm{Gal}(K/F)$ è normale in $\mathrm{Gal}(K/k)$. Mostriamo prima che per ogni $\sigma \in \mathrm{Gal}(K/k)$ si ha che $\sigma_{|F} \in \mathrm{Gal}(F/k)$. La mappa $\sigma_{|F} : F \longrightarrow \sigma(F)$ è chiaramente un omomorfismo di gruppi iniettivo che lascia fissi gli elementi di k, rimane da verificare che $\sigma(F) = F$. Poiché $F \supseteq k$ è una estensione normale si ha che $\sigma(F) \subseteq F$. Proviamo che $F \subseteq \sigma(F)$. Se $x \in F$ allora esiste y in K tale che $\sigma(y) = x$ allora $y = \sigma^{-1}(x)$, ma σ^{-1} è un automorfismo che fissa k quindi necessariamente $y \in F$.
Consideriamo il seguente omomorfismo di gruppi

$$\begin{array}{rccc} \phi: & \mathrm{Gal}(K/k) & \longrightarrow & \mathrm{Gal}(F/k) \\ & \sigma & \longmapsto & \sigma_{|F}. \end{array}$$

Si ha che

$$\ker \phi = \{\sigma \in \mathrm{Gal}(K/k) \text{ tali che } \sigma_{|F} = id_F\} = \mathrm{Gal}(K/F)$$

quindi $\mathrm{Gal}(K/F)$ è normale in $\mathrm{Gal}(K/k)$.
Siano $\mathrm{Gal}(K/F_1), \mathrm{Gal}(K/F_2)$ tali che F_1, $F_2 \in \mathcal{F}$, vogliamo dimostrare che esiste $F_3 \in \mathcal{F}$ tale che $\mathrm{Gal}(K/F_3) \subseteq \mathrm{Gal}(K/F_1) \cap \mathrm{Gal}(K/F_2)$. Poiché $F_1 \supseteq k$ è una estensione finita di Galois si ha che esiste $\alpha_1 \in F_1$ separabile tale che $F_1 = k(\alpha_1)$. Analogamente esiste $\alpha_2 \in F_2$ separabile tale che $F_2 = k(\alpha_2)$. Siano p_{α_1} il polinomio minimo di α_1 su k e p_{α_2} il polinomio minimo di α_2 su k. Se p_{α_1} e p_{α_2} sono distinti allora non sono multipli l'uno dell'altro. Poiché p_{α_1} e p_{α_2} sono irriducibili e separabili si ha che $p_{\alpha_1} \cdot p_{\alpha_2}$ è separabile. Sia F_3 il campo di spezzamento di $p_{\alpha_1} \cdot p_{\alpha_2}$. Poiché F_3 è il campo di spezzamento di un polinomio separabile per il Teorema 6.7 si ha che $F_3 \supseteq k$ è di Galois. Poiché $K \supseteq k$ è normale si ha che $K \supseteq F_3$ dunque $F_3 \in \mathcal{F}$. Inoltre F_3 contiene F_1 e F_2 quindi $\mathrm{Gal}(K/F_3)$ contiene sia $\mathrm{Gal}(K/F_1)$ che $\mathrm{Gal}(K/F_2)$.

Osservazione 6.9. *Se $F \supseteq k$ è una estensione di campi finita e di Galois allora in $\mathrm{Gal}(F/k)$ la topologia precedentemente definita coincide con la topologia discreta.*

Dimostrazione. Poiché l'estensione $F \supseteq k$ è finita e di Galois si ha che $\mathrm{Gal}(F/F) = \{id_F\}$ è un aperto per $\mathrm{Gal}(F/k)$. Poiché $\mathrm{Gal}(F/k)$ è un gruppo topologico, per ogni automorfismo $\sigma \in \mathrm{Gal}(F/k)$ si ha che $\sigma \circ \{id_F\}$ è aperto.

□

Lemma 6.10. *Sia $\{K_i\}_{i \in I}$ una famiglia di campi tali che $K \supseteq K_i \supseteq k$ e l'estensione $K_i \supseteq k$ è finita. Se $K = \bigcup_{i \in I} K_i$ allora $\{\sigma \circ \mathrm{Gal}(K/K_i)$ con $\sigma \in \mathrm{Gal}(K/k)$ e $i \in I\}$ è una base per la topologia di $\mathrm{Gal}(K/k)$.*

Dimostrazione. Proviamo che per ogni i si ha che $\mathrm{Gal}(K/K_i)$ è aperto in $\mathrm{Gal}(K/k)$. Sia $i \in I$, mostriamo che esiste $N \in \mathcal{F}$ con $N \supseteq K_i$. Il ragionamento è simile a quello fatto per dimostrare che $\{\mathrm{Gal}(K/F)$ con $F \in \mathcal{F}\}$ è una base filtro, rivediamolo brevemente senza l'uso del teorema dell'elemento primitivo. Sia $K_i = k(\alpha_1, \ldots, \alpha_n)$. Consideriamo

p_{α_j} polinomio minimo di α_j su k per ogni $j = 1, \ldots, n$. Sia N il campo di spezzamento di $p_{\alpha_1} \cdot \ldots \cdot p_{\alpha_n}$. Si ha

$$K \supseteq N \supseteq k(\alpha_1, \ldots, \alpha_n) \supseteq k$$

dunque $N \in \mathcal{F}$.
Abbiamo quindi che $\mathrm{Gal}(K/N)$ è un sottogruppo di $\mathrm{Gal}(K/K_i)$ dunque per l'osservazione 2.2 punto d) si ha che $\mathrm{Gal}(K/K_i)$ è un aperto di $\mathrm{Gal}(K/k)$.
Proviamo che se $N \in \mathcal{F}$ allora esiste $i \in I$ tale che $\mathrm{Gal}(K/K_i) \subseteq \mathrm{Gal}(K/N)$. Se questo vale si ha che

$$\mathrm{Gal}(K/N) = \bigcup_{\sigma \in \mathrm{Gal}(K/N)} \sigma \mathrm{Gal}(K/K_i),$$

dunque per ogni $g \in \mathrm{Gal}(K/k)$ si ha che

$$g\mathrm{Gal}(K/N) = \bigcup_{\sigma \in \mathrm{Gal}(K/N)} (g \circ \sigma)\mathrm{Gal}(K/K_i)$$

quindi $\{\sigma \circ \mathrm{Gal}(K/K_i) \text{ con } i \in I \text{ e } \sigma \in \mathrm{Gal}(K/k)\}$ è una base per la topologia di $\mathrm{Gal}(K/k)$.
Sia $N \in \mathcal{F}$ per il teorema dell'elemento primitivo esiste $\alpha \in N$ separabile tale che $N = k(\alpha)$. In particolare $\alpha \in K$ dunque esiste un $i \in I$ tale che $\alpha \in K_i$. Poiché N è il più piccolo campo contenente k e α si ha che $N \subseteq K_i$ dunque $\mathrm{Gal}(K/K_i) \subseteq \mathrm{Gal}(K/N)$.
□

Lemma 6.11. *Siano X un gruppo e Y, H due suoi sottogruppi. Sia x un elemento di X tale che $(xH) \cap Y \neq \emptyset$. Allora esiste $y \in Y$ tale che $(xH) \cap Y = y(Y \cap H)$.*

Dimostrazione. Se $(xH) \cap Y \neq \emptyset$ esistono $y \in Y$ e $h \in H$ tali che $y = xh$ allora $yH = xH$. Quindi $(xH) \cap Y = (yH) \cap Y$ che risulta essere uguale a $y(H \cap Y)$.
□

Proposizione 6.12. *Sia $K = \bigcup_{i \in I} F_i$ con $F_i \supseteq k$ estensione finita di Galois. Se vale che per ogni $i, j \in I$ esiste $m \in I$ tale che F_m contiene sia F_i che F_j allora*

1) *$(\mathrm{Gal}(F_i/k), \varphi_{ij})$ è un sistema inverso indicizzato da I, dove se F_i è un sottocampo di F_j*

$$\begin{array}{rccc} \varphi_{ij}: & \mathrm{Gal}(F_j/k) & \longrightarrow & \mathrm{Gal}(F_i/k) \\ & \sigma & \longmapsto & \sigma_{|F_i}. \end{array}$$

2) *$\mathrm{Gal}(K/k)$ è isomorfo come gruppo topologico a $\varprojlim_{i \in I} \mathrm{Gal}(F_i/k)$.*

Dimostrazione. I è un insieme diretto con la relazione $\leq'$ dove $i \leq' j$ se e solo se F_i è un sottocampo di F_j. Analogamente a come fatto per la topologia di $\mathrm{Gal}(K/k)$ si dimostra che se F_i è un sottocampo di F_j si ha che per ogni $\sigma \in \mathrm{Gal}(F_j/k)$ vale che $\sigma_{|F_i} \in \mathrm{Gal}(F_i/k)$. Il fatto che $(\mathrm{Gal}(F_i/k), \varphi_{ij})$ sia un sistema inverso è una semplice verifica.
Sia

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(K/k) & \longrightarrow & s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k) \\ & \sigma & \longmapsto & (\sigma_{|F_i})_{i\in I} \end{array}$$

Per ogni $\sigma \in \mathrm{Gal}(K/k)$ si ha che $(\sigma_{|F_i})_{i\in I} \in s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k)$, infatti per ogni $r \leq' s$ si ha

$$\varphi_{rs} \circ p_s((\sigma_{|F_i})_{i\in I}) = \varphi_{rs}(\sigma_{|F_s}) = \sigma_{|F_r} = p_r((\sigma_{|F_i})_{i\in I}).$$

Si verifica facilmente che φ è un omomorfismo di gruppi. Costruiamo ora l'applicazione inversa di φ. Sia

$$\begin{array}{rccc} \psi: & s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k) & \longrightarrow & \mathrm{Gal}(K/k) \\ & (\sigma_{F_i})_{i\in I} & \longmapsto & \psi\left((\sigma_{F_i})_{i\in I}\right): \begin{array}{ccc} K & \longrightarrow & K \\ \alpha & \longmapsto & \sigma_{F_s}(\alpha) \end{array} \end{array}$$

dove F_s è tale che $s \in I$ e $\alpha \in F_s$ (per ipotesi un tale F_s esiste sempre). Mostriamo che $\psi((\sigma_{F_i})_{i\in I})(\alpha)$ non dipende dalla scelta di s. Siano s ed r tali che $\alpha \in F_s, F_r$. Per ipotesi esiste F_t contenente sia F_s che F_r. Poiché $(\sigma_{F_i})_{i\in I} \in s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k)$ si ha che $(\varphi_{st} \circ p_t)((\sigma_{F_i})_{i\in I}) = p_s((\sigma_{F_i})_{i\in I})$ e $(\varphi_{rt} \circ p_t)((\sigma_{F_i})_{i\in I}) = p_r((\sigma_{F_i})_{i\in I})$. Allora $\varphi_{st}(\sigma_{F_t}) = \sigma_{F_t|F_s} = \sigma_{F_s}$ e $\sigma_{F_t|F_r} = \sigma_{F_r}$. Dunque $\sigma_{F_s}(\alpha) = \sigma_{F_t}(\alpha) = \sigma_{F_r}(\alpha)$.
Proviamo che $\psi\left((\sigma_{F_i})_{i\in I}\right)$ è suriettiva. Vogliamo far vedere che per ogni $\beta \in K$ esiste $\alpha \in K$ tale che $\sigma_{F_s}(\alpha) = \beta$ dove $\alpha \in F_s$. Sia s tale che $\beta \in F_s$, allora $\sigma_{F_s}^{-1}(\beta) =: \alpha \in F_s$.
Proviamo che $\psi\left((\sigma_{F_i})_{i\in I}\right)$ è iniettiva. Se si ha che $\psi\left((\sigma_{F_i})_{i\in I}\right)(\alpha) = \sigma_{F_s}(\alpha)$ è uguale a $\psi\left((\sigma_{F_i})_{i\in I}\right)(\beta) = \sigma_{F_r}(\beta)$ allora $\sigma_{F_s}(\alpha) = \sigma_{F_r}(\beta) \in F_s \cap F_r$. Poiché $(\sigma_{F_i})_{i\in I}^{-1} = (\sigma_{F_i}^{-1})_{i\in I}$ appartiene $s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k)$ si ha che $\sigma_{F_s}^{-1}$ e $\sigma_{F_r}^{-1}$ coincidono nell'intersezione dei loro domini. Quindi $\sigma_{F_s}^{-1}(\sigma_{F_s}(\alpha)) = \sigma_{F_r}^{-1}(\sigma_{F_r}(\beta))$ allora $\alpha = \beta$.
Proviamo che $\psi\left((\sigma_{F_i})_{i\in I}\right)$ è un omomorfismo di anelli. Mostriamo ad esempio che per ogni $\alpha_1, \alpha_2 \in K$ si ha che

$$\psi\left((\sigma_{F_i})_{i\in I}\right)(\alpha_1 \cdot \alpha_2) = \sigma_{F_s}(\alpha_1 \cdot \alpha_2) = \psi\left((\sigma_{F_i})_{i\in I}\right)(\alpha_1) \cdot \psi\left((\sigma_{F_i})_{i\in I}\right)(\alpha_2) = \sigma_{F_r}(\alpha_1) \cdot \sigma_{F_t}(\alpha_2),$$

dove s è tale che $\alpha_1 \cdot \alpha_2 \in F_s$, r è tale che $\alpha_1 \in F_r$ e t è tale che $\alpha_2 \in F_t$. Se consideriamo $F_m \supseteq F_r, F_t$ si ha $\sigma_{F_s}(\alpha_1\alpha_2) = \sigma_{F_m}(\alpha_1\alpha_2) = \sigma_{F_m}(\alpha_1)\sigma_{F_m}(\alpha_2) = \sigma_{F_r}(\alpha_1)\sigma_{F_t}(\alpha_2)$. Dunque per ogni $(\sigma_{F_i})_{i\in I} \in s\varprojlim_{i\in I} \mathrm{Gal}(F_i/k)$ si ha che $\psi\left((\sigma_{F_i})_{i\in I}\right) \in \mathrm{Gal}(K/k)$.
Si ha inoltre che

$$(\varphi \circ \psi)\left((\sigma_{F_i})_{i\in I}\right) = \varphi(\alpha \longmapsto \sigma_{F_s}(\alpha)) = \left((\alpha \longmapsto \sigma_{F_s}(\alpha))_{|F_i}\right)_{i\in I} = (\sigma_{F_i})_{i\in I}$$

$$(\psi \circ \varphi)(\sigma) = \psi\left((\sigma_{|F_i})_{i\in I}\right) = \alpha \longmapsto \sigma_{|F_s}(\alpha) = \sigma.$$

Dunque abbiamo provato che φ è un isomorfismo di gruppi.
Proviamo ora che φ è aperta. Mostriamo che φ è aperta sugli insiemi $\mathrm{Gal}(K/F_i)$ per ogni $i \in I$. Se vale che $\varphi(\mathrm{Gal}(K/F_i))$ è un aperto per ogni i allora per ogni $\sigma \in \mathrm{Gal}(K/k)$ si ha che $\varphi(\sigma\mathrm{Gal}(K/F_i)) = \varphi(\sigma) \circ \varphi(\mathrm{Gal}(K/F_i))$ è aperto e quindi φ è aperta su di una base di $\mathrm{Gal}(K/k)$, dunque è aperta. Mostriamo che

$$\varphi(\mathrm{Gal}(K/F_s)) = \{(\sigma_{F_i})_{i\in I} \in s\varprojlim \mathrm{Gal}(F_i/k) \text{ tale che } \sigma_{F_s} = id_{F_s}\} := A.$$

Chiaramente per ogni $\sigma \in \mathrm{Gal}(K/F_s)$ si ha che $\varphi(\sigma) \in A$. Se $(\sigma_{F_i})_{i\in I} \in A$ sia $\sigma = \varphi^{-1}((\sigma_{F_i})_{i\in I})$. Si ha che $\sigma \in \mathrm{Gal}(K/F_s)$ poiché $\sigma_{|F_s} = \sigma_{F_s} = id_{F_s}$.
A è un aperto di $s\varprojlim \mathrm{Gal}(F_i/k)$ infatti $A = s\varprojlim \mathrm{Gal}(F_i/k) \cap \prod_{\substack{i\in I\\ i\neq s}} \mathrm{Gal}(F_i/k) \times id_{F_s}$ e $\prod_{i\in I} \mathrm{Gal}(F_i/k) \times id_{F_s}$ è un aperto di $\prod_{i\in I} \mathrm{Gal}(F_i/k)$ poiché in $\mathrm{Gal}(F_s/k)$ abbiamo la topologia discreta.
Mostriamo che φ è continua. Poiché una base per $\prod_{i\in I} \mathrm{Gal}(F_i/k)$ è data da

$$g \circ \Big(\prod_{\substack{i\in I\\ i\neq i_1,\ldots,i_n}} \mathrm{Gal}(F_i/k) \times \prod_{j=1}^{n} id_{F_{i_j}} \Big)$$

dove $g \in \prod_{i\in I} \mathrm{Gal}(F_i/k)$, basta dimostrare che la retroimmagine tramite φ di

$$s\varprojlim \mathrm{Gal}(F_i/k) \cap g \circ \Big(\prod_{\substack{i\in I\\ i\neq i_1,\ldots,i_n}} \mathrm{Gal}(F_i/k) \times \prod_{j=1}^{n} id_{F_{i_j}} \Big)$$

è aperto.

Poniamo $Y := s\varprojlim \mathrm{Gal}(F_i/k)$ e $H := \prod_{\substack{i\in I\\ i\neq i_1,\ldots,i_n}} \mathrm{Gal}(F_i/k) \times \prod_{j=1}^{n} id_{F_{i_j}}$.
Per il Lemma 6.11 dobbiamo provare che $\varphi^{-1}(y(Y \cap H))$ è aperto in $\mathrm{Gal}(K/k)$ per ogni $y \in Y$. Poiché φ è un isomorfismo di gruppi si ha che $\varphi^{-1}(y(Y\cap H)) = \varphi^{-1}(y)\varphi^{-1}(Y\cap H)$, se proviamo che $\varphi(Y \cap H)$ è aperto in $\mathrm{Gal}(K/k)$ abbiamo concluso. Ma $\varphi^{-1}(Y \cap H) = = \mathrm{Gal}(K/F_{i_1}) \cap \ldots \cap \mathrm{Gal}(K/F_{i_n})$ che è un aperto di $\mathrm{Gal}(K/k)$.

□

Corollario 6.13. $\mathrm{Gal}(K/k) \cong \varprojlim_{F\in\mathcal{F}} \mathrm{Gal}(F/k)$.

Dimostrazione. Se $K = \bigcup_{F \in \mathcal{F}} F$ e per ogni $F_i, F_j \in \mathcal{F}$ si ha che esiste $F_m \in \mathcal{F}$ tale che $F_m \supseteq F_i, F_j$ per la Proposizione 6.12 abbiamo concluso. Abbiamo già dimostrato che se $F_i, F_j \in \mathcal{F}$ allora esiste $F_m \in \mathcal{F}$ tale che $F_m \supseteq F_i, F_j$. Mostriamo che $K \subseteq \bigcup_{F \in \mathcal{F}} F$. Se $\alpha \in K$ allora il polinomio minimo p_α di α su k ha tutte le radici in K e sono a due a due distinte. Siano tali radici $\alpha, \alpha_1, \ldots, \alpha_n$. Si ha che $k(\alpha, \alpha_1, \ldots, \alpha_n)$ è il campo di spezzamento di un polinomio separabile dunque $\alpha \in k(\alpha, \alpha_1, \ldots, \alpha_n) \in \mathcal{F}$.

□

Lemma 6.14. *Siano Y un gruppo, H un insieme, y un elemento di Y. Allora vale che $y(Y \cap H) = (yH) \cap Y$.*

Dimostrazione. Si ha che $y(Y \cap H) \subseteq (yH) \cap Y$ poiché Y è un gruppo. Se $yH \cap Y$ è uguale all'insieme vuoto allora anche $y(Y \cap H)$ è uguale all'insieme vuoto e quindi i due insiemi sono uguali. Se $(yH) \cap Y \neq \emptyset$ allora esistono $z \in Y$ ed un $h \in H$ tale che $z = yh$ dunque poiché Y è un gruppo $h \in Y$ allora $z \in y(Y \cap H)$.

□

Proposizione 6.15. *Sia M un campo tale che $K \supseteq M \supseteq k$. Poiché $K \supseteq M$ è una estensione algebrica e di Galois si può dotare* $\mathrm{Gal}(M/k)$ *della topologia precedentemente definita. Poiché* $\mathrm{Gal}(K/M)$ *è un sottogruppo di* $\mathrm{Gal}(K/k)$ *si può dotare* $\mathrm{Gal}(K/M)$ *della topologia indotta da* $\mathrm{Gal}(K/k)$*. Vale che queste due topologie su* $\mathrm{Gal}(K/M)$ *coincidono.*

Dimostrazione. Mostriamo che le due topologie hanno una stessa base.
Una base per $\mathrm{Gal}(K/M)$ come topologia indotta è data da insiemi della forma $(\sigma \circ \mathrm{Gal}(K/L)) \cap \mathrm{Gal}(K/M)$ al variare di $\sigma \in \mathrm{Gal}(K/k)$ e $L \in \mathcal{F}$ (cioè L tale che $K \supseteq L \supseteq k$ e $L \supseteq k$ è finita e di Galois).
Sia LM il più piccolo sottocampo di K contenente sia L che M. Chiaramente vale che $K \supseteq LM \supseteq k$. Si ha che LM è una estensione finita di M per ogni $L \in \mathcal{F}$. Poiché $K = \bigcup_{L \in \mathcal{F}} L$ allora vale anche che $K = \bigcup_{L \in \mathcal{F}} LM$. Per il Lemma 6.10 si ha che gli insiemi del tipo $\tau\mathrm{Gal}(K/LM)$ al variare di $\tau \in \mathrm{Gal}(K/M)$ e di $L \in \mathcal{F}$ formano una base per $\mathrm{Gal}(K/M)$ come gruppo di Galois.
Per ogni $L \in \mathcal{F}$ si ha che $\mathrm{Gal}(K/M) \cap \mathrm{Gal}(K/L) = \mathrm{Gal}(K/LM)$.
Se $A = \tau\mathrm{Gal}(K/LM) = \tau\left(\mathrm{Gal}(K/M) \cap \mathrm{Gal}(K/L)\right)$ con $\tau \in \mathrm{Gal}(K/M)$ e $L \in \mathcal{F}$ si ha per il Lemma 6.14 che $A = (\tau\mathrm{Gal}(K/L)) \cap \mathrm{Gal}(K/M)$.
Se $\emptyset \neq A = (\sigma\mathrm{Gal}(K/L)) \cap \mathrm{Gal}(K/M)$ con $\sigma \in \mathrm{Gal}(K/k)$ e $L \in \mathcal{F}$ allora per il Lemma 6.11 esiste $\tau \in \mathrm{Gal}(K/M)$ tale che $A = \tau(\mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/M)) = \tau(\mathrm{Gal}(K/LM))$.

□

Osservazione 6.16. *Siano $N \supseteq k$ una estensione di Galois finita e $R_1 \supseteq k$, $R_2 \supseteq k$ due estensioni di campi finite tali che sia R_1 che R_2 siano inclusi in N. Sia $\gamma : R_1 \longrightarrow R_2$*

un isomorfismo di campi che fissa k. Allora esiste un automorfismo $\phi : N \longrightarrow N$ tale che $\phi_{|R_1} = \gamma$.

Dimostrazione. Vogliamo utilizzare la Proposizione 6.2. Poiché $N \supseteq k$ è una estensione di Galois per il teorema dell'elemento primitivo si ha che esiste $\alpha \in N$ tale che $N = k(\alpha)$. Sia $p_\alpha^{R_1}$ il polinomio minimo di α su R_1. Dato che $N \supseteq k$ è di Galois allora anche $N \supseteq R_1$ è di Galois quindi $p_\alpha^{R_1}$ ha tutte le radici contenute in N. Se M è un altro campo contenenente R_1 e tutte le radici di $p_\alpha^{R_1}$ allora in particolare $\alpha \in M$ quindi $M \supseteq R_1(\alpha) \supseteq k(\alpha) = N$. Dunque N è un campo di spezzamento per $p_\alpha^{R_1}$.
Sia $\tilde{\gamma}$ la mappa definita nella Proposizione 6.2. Si verifica facilmente che $\tilde{\gamma}$ è un isomorfismo di anelli. Sia F un campo di spezzamento di $\tilde{\gamma}(p_\alpha^{R_1})$ su R_2. Sia $p_\alpha^k \in k[x] \subseteq R_1[x]$ il polinomio minimo di α su k. Esiste $q \in R_1[x]$ tale che $p_\alpha^k = p_\alpha^{R_1} \cdot q$, quindi dato che γ fissa k si ha che $\tilde{\gamma}(p_\alpha^k) = p_\alpha^k = \tilde{\gamma}(p_\alpha^{R_1}) \cdot \tilde{\gamma}(q)$. Dunque le radici di $\tilde{\gamma}(p_\alpha^{R_1})$ sono contenute nell'insieme delle radici di p_α^k, quindi sono tutte contenute in N. Allora F è contenuto in N. Per la Proposizione 6.2 si ha che esiste un isomorfismo di campi $\phi : N \longrightarrow F$ tale che $\phi_{|R_1} = \gamma$. I campi N ed F sono entrambi spazi vettoriali su k e poiché ϕ fissa k si ha che ϕ è anche un isomorfismo di spazi vettoriali su k. In particolare F ed N hanno la stessa dimensione su k. Poiché F è contenuto in N si ha quindi che $F = N$.

□

Proposizione 6.17. *Siano M_1, M_2 due campi intermedi di $K \supseteq k$ e sia $\gamma : M_1 \to M_2$ un isomorfismo di campi che fissa ogni elemento di k. Allora γ può essere esteso ad un automorfismo di K.*

Dimostrazione. Per ogni $N \in \mathcal{F}$ sia

$$B_N := \{(\sigma_F)_{F\in\mathcal{F}} \in \prod_{F\in\mathcal{F}} \mathrm{Gal}(F/k) \text{ t.c. } \sigma_{N|N\cap M_1} = \gamma_{|N\cap M_1} \text{ e } \sigma_L = \sigma_{N|L} \text{ per ogni } L \subseteq N\}.$$

Proviamo che per ogni $N \in \mathcal{F}$ si ha che B_N è diverso dal vuoto. Consideriamo la mappa $\gamma_{|M_1\cap N} : M_1 \cap N \longrightarrow \gamma(M_1 \cap N)$. Mostriamo che $\gamma(M_1 \cap N) \subseteq N$. Poiché $M_1 \cap N \supseteq k$ è una estensione finita allora esistono $\alpha_1, \ldots, \alpha_n \in M_1 \cap N$ tali che $M_1 \cap N = k(\alpha_1, \ldots, \alpha_n)$. Dato che $\alpha_1, \ldots, \alpha_n \in N$ si ha che $\alpha_1, \ldots, \alpha_n$ sono separabili quindi per il teorema dell'elemento primitivo esiste $\alpha \in M_1 \cap N$ tale che $M_1 \cap N = k(\alpha)$. Consideriamo p_α^k il polinomio minimo di α su k. Poiché γ fissa k si ha che $\gamma(\alpha) \in K$ è una radice di p_α^k. Quindi $\gamma(\alpha) \in N$, allora $\gamma(M_1 \cap N) \subseteq N$.
Per l'Osservazione 6.16 esiste un automorfismo $\phi : N \longrightarrow N$ tale che $\phi_{|M_1\cap N} = \gamma_{|M_1\cap N}$. Definiamo $(\sigma_F)_{F\in\mathcal{F}}$ nel seguente modo: $\sigma_N := \phi$, $\sigma_L := \sigma_{N|L}$ per ogni $L \in \mathcal{F}$ tale che $L \subseteq N$, $\sigma_F = \mathrm{id}_F$ altrimenti. Questo elemento così costruito appartiene a B_N.
Si ha che B_N è un chiuso di $\prod_{F\in\mathcal{F}} \mathrm{Gal}(F/k)$, infatti

$$B_N = \{(\sigma_F)_{F\in\mathcal{F}} \text{ tali che } \sigma_{N|M_1\cap N} = \gamma_{|M_1\cap N}\} \bigcap_{L\in\mathcal{F} \text{ t.c. } L\subseteq N} \{(\sigma_F)_{F\in\mathcal{F}} \text{ tali che } \sigma_L = \sigma_{N|L}\}$$

che è una intersezione di chiusi di $\prod_{F\in\mathcal{F}} \mathrm{Gal}(F/k)$.
Proviamo che ogni intersezione finita di insiemi del tipo B_N con $N \in \mathcal{F}$ non è vuota. Siano $N_1, \ldots, N_n \in \mathcal{F}$. Poiché $N_i \supseteq k$ è di Galois si ha che esiste $\alpha_i \in N_i$ separabile tale che $N_i = k(\alpha_i)$. Sia M il campo di spezzamento su k del prodotto dei polinomi minimi degli α_i su k. Come già osservato quando abbiamo definito una topologia per i gruppi di Galois, $M \in \mathcal{F}$ e contiene ogni N_i. Per l'Osservazione 6.16 esiste un automorfismo $\phi : M \longrightarrow M$ tale che $\phi_{|M\cap M_1} = \gamma_{|M\cap M_1}$. Poniamo $\sigma_{N_i} := \phi_{|N_i}$, allora $\sigma_{N_i|N_i\cap M_1} = \phi_{|N_i\cap M_1} = \gamma_{|N_i\cap M_1}$ dato che $N_i \cap M_1 \subseteq M \cap M_1$ per ogni $i = 1, \ldots, n$. Per ogni i, se $L \in \mathcal{F}$ è tale che $L \subseteq N_i$ poniamo $\sigma_L := \sigma_{N_i|L}$. Si noti che se L è contenuto in diversi N_i non c'è ambiguità nella definizione, infatti se $x \in L \subseteq N_{i_1} \cap N_{i_2}$ si ha che $\sigma_L(x) = \sigma_{N_{i_1}}(x) = \phi(x) = \sigma_{N_{i_2}}(x)$. Poniamo i restanti elementi del prodotto cartesiano $\prod_{F\in\mathcal{F}} \mathrm{Gal}(F/k)$ uguali alla rispettiva identità. Questo elemento così costruito appartiene a $B_{N_1} \cap \ldots \cap B_{N_n}$.
Per ogni $F \in \mathcal{F}$ si ha che $\mathrm{Gal}(F/k)$ è quasi compatto poiché discreto, allora per il Teorema di Tychonoff $\prod_{F\in\mathcal{F}} \mathrm{Gal}(F/k)$ è quasi compatto. Se $\bigcap_{N\in\mathcal{F}} B_N = \emptyset$ allora esistono $B_{i_1}, \ldots, B_{i_n}$ tali che $B_{1_1} \cap \ldots \cap B_{i_n} = \emptyset$, che è assurdo. Dunque $\bigcap_{F\in\mathcal{F}} B_N \neq \emptyset$.
Mostriamo che $\bigcap_{F\in\mathcal{F}} B_N \subseteq s\lim_{\longleftarrow F\in\mathcal{F}}(\mathrm{Gal}(F/k))$. Per ogni $(\sigma_F)_{F\in\mathcal{F}} \in \bigcap_{F\in\mathcal{F}} B_N$ se N_i è un sottocampo di N_j si ha che $(\sigma_F)_{F\in\mathcal{F}} \in B_{n_j}$ quindi $(\varphi_{ij} \circ p_j)((\sigma_F)_{F\in\mathcal{F}}) = \varphi_{ij}(\sigma_{N_j}) = = \sigma_{N_j|N_i} = \sigma_{N_i} = p_i((\sigma_F)_{F\in\mathcal{F}})$ con le notazioni utilizzate nella Proposizione 6.12.
Sia $(\sigma_F)_{F\in\mathcal{F}} \in \bigcap_{N\in\mathcal{F}} B_N$. Consideriamo la mappa ψ definita nella dimostrazione della Proposizione 6.12. Si ha che

$$\begin{array}{rccc} \psi((\sigma_F)_{F\in\mathcal{F}}) : & K & \longrightarrow & K \\ & \alpha & \longmapsto & \sigma_{F_s}(\alpha) \end{array}$$

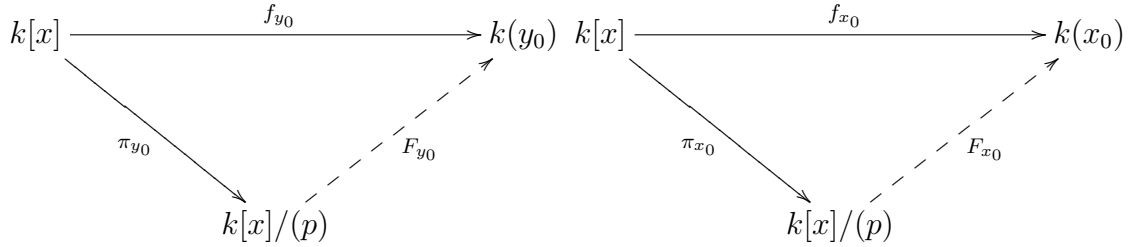
appartiene $\mathrm{Gal}(K/k)$. Se $\alpha \in M_1$ esiste s tale che $F_s \in \mathcal{F}$ e $\alpha \in M_1 \cap F_s$ e si ha che $\sigma_{F_s}(\alpha) = \gamma(\alpha)$ poiché $(\sigma_F)_{F\in\mathcal{F}} \in B_{F_s}$. Allora $\psi((\sigma_F)_{F\in\mathcal{F}})$ è un automorfismo di K che estende γ.

□

Lemma 6.18. *Sia $F \supseteq k$ una estensione di campi algebrica. Siano x_0 un elemento di F e p il suo polinomio minimo su k. Supponiamo che p abbia grado maggiore di uno e che y_0 sia una sua altra radice contenuta nel suo campo di spezzamento su k. Allora esiste un isomorfismo da $k(x_0)$ a $k(y_0)$ che fissa k e manda x_0 in y_0.*

Dimostrazione. Poiché x_0 e y_0 sono algebrici su k allora $k(x_0) = k[x_0]$ e $k(y_0) = k[y_0]$.

Consideriamo i due seguenti noti diagrammi commutativi



dove per ogni $a_0 + a_1x + \ldots + a_nx^n \in k[x]$ si ha che $f_{y_0}(a_0 + a_1x + \ldots + a_nx^n) = = a_0 + a_1y_0 + \ldots + a_ny_0^n$ e $f_{x_0}(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1x_0 + \ldots + a_nx_0^n$; le mappe π_{y_0} e π_{x_0} sono mappe quoziente e le mappe F_{y_0} e F_{x_0} sono le mappe indotte. Poiché $k(x_0) = k[x_0]$ e $k(y_0) = k[y_0]$ si ha che le mappe f_{y_0} e f_{x_0} sono suriettive dunque F_{y_0} e F_{x_0} sono isomorfismi di campi. Quindi la seguente composizione di isomorfismi di campi

$$\begin{array}{ccccccc} k(x_0) & \xrightarrow{F_{x_0}^{-1}} & k[x]/(p) & \xrightarrow{F_{y_0}} & k(y_0) \\ a_0 + a_1x_0 + \ldots + a_nx_0^n & \longmapsto & a_0 + a_1x_0 + \ldots + a_nx_0^n + (p) & \longmapsto & a_0 + a_1y_0 + \ldots + a_ny_0^n \end{array}$$

è un isomorfismo di campi che fissa k e manda x_0 in y_0.

□

Si ricorda la seguente notazione: se G è un gruppo topologico e H è un sottoinsieme di G, con $H \leq G$ si intenderà che H è un sottogruppo chiuso di G.

Teorema 6.19. *Vale che*

$$\begin{array}{rccc} \phi: & \{\textit{campi } M \textit{ tali che } K \supseteq M \supseteq k\} & \longrightarrow & \{H \textit{ tali che } H \leq \mathrm{Gal}(K/k)\} \\ & M & \longmapsto & \mathrm{Gal}(K/M) \end{array}$$

è una biezione che rovescia le inclusioni. Si ha inotre che la mappa inversa di ϕ è

$$\begin{array}{rccc} \phi^{-1}: & \{H \textit{ tali che } H \leq \mathrm{Gal}(K/k)\} & \longrightarrow & \{\textit{campi } M \textit{ tali che } K \supseteq M \supseteq k\} \\ & H & \longmapsto & K^H. \end{array}$$

Dimostrazione. Mostriamo subito che se M è tale che $K \supseteq M \supseteq k$ allora $\mathrm{Gal}(K/M)$ è un sottogruppo chiuso di $\mathrm{Gal}(K/k)$. Sia $\Lambda = \{\lambda \text{ tali che } M \supseteq S_\lambda \supseteq k \text{ con } S_\lambda \supseteq k \text{ finita}\}$. Si ha che $M = \bigcup_{\lambda \in \Lambda} S_\lambda$ poiché se $\alpha \in M$ allora $k(\alpha) = S_{\lambda_0}$ per un certo $\lambda_0 \in \Lambda$. Per ogni λ si ha che l'estensione $S_\lambda \supseteq k$ è finita quindi, poiché $K \supseteq k$ è di Galois, esiste una estensione $F_\lambda \supseteq k$ finita di Galois tale che $F_\lambda \supseteq S_\lambda$, dunque $\mathrm{Gal}(K/F_\lambda) \subseteq \mathrm{Gal}(K/S_\lambda)$. Poiché $\mathrm{Gal}(K/F_\lambda)$ è un aperto di $\mathrm{Gal}(K/k)$ anche $\mathrm{Gal}(K/S_\lambda)$ è un aperto di $\mathrm{Gal}(K/k)$ per ogni λ. Inoltre $\mathrm{Gal}(K/M) = \bigcap \mathrm{Gal}(K/S_\lambda)$, quindi $\mathrm{Gal}(K/M)$ è un chiuso di $\mathrm{Gal}(K/k)$.

Risulta chiaro che per ogni $H \leq \mathrm{Gal}(K/k)$ si ha che $K \supseteq K^H \supseteq k$. Si verifica facilmente che se $M_1 \subseteq M_2$ allora $\phi(M_1) = \mathrm{Gal}(K/M_1) \supseteq \mathrm{Gal}(K/M_2) = \phi(M_2)$.
Proviamo che $(\phi^{-1} \circ \phi)(M) = M$ per ogni M campo intermedio fra K e k. Dobbiamo quindi mostrare che $\phi^{-1}(\mathrm{Gal}(K/M)) = K^{\mathrm{Gal}(K/M)} = M$ per ogni M. Chiaramente $M \subseteq K^{\mathrm{Gal}(K/M)}$.
Proviamo che $M \supseteq K^{\mathrm{Gal}(K/M)}$. Sia $x_0 \in K^{\mathrm{Gal}(K/M)}$, se per assurdo $x_0 \in K \setminus M$ allora, poiché K è algebrica su k e quindi è anche algebrica su M, si ha che esiste $p^M_{x_0}$ polinomio minimo di x_0 su M. Il grado di $p^M_{x_0}$ è maggiore di uno altrimenti $x \in M$. Sia $y_0 \in K$ un'altra radice di $p^M_{x_0}$ nel suo campo di spezzamento su M. Poiché $K \supseteq k$ è separabile il polinomio minimo $p^k_{x_0}$ di x_0 su k ha tutte le radici distinte nel suo campo di spezzamento su k. Dato che $p^M_{x_0} | p^k_{x_0}$ le radici di $p^M_{x_0}$ sono tutte distinte quindi $x_0 \neq y_0$. Per il Lemma 6.18 esiste un isomorfismo fra $M(x_0)$ e $M(y_0)$ che lascia fisso M e manda x_0 in y_0. Per la Proposizione 6.17 tale isomorfismo può essere esteso ad un automorfismo σ da K in K. Chiaramente $\sigma \in \mathrm{Gal}(K/M)$. Ma $\sigma(x_0) = y_0 \neq x_0$ quindi $x_0 \notin K^{\mathrm{Gal}(K/M)}$ che è assurdo. Dunque per ogni campo intermedio M fra K e k si ha che $(\phi^{-1} \circ \phi)(M) = M$.
Proviamo ora che $(\phi \circ \phi^{-1})(H) = H$ per ogni $H \leq \mathrm{Gal}(K/k)$, cioè che $\mathrm{Gal}(K/K^H) = H$ per ogni $H \leq \mathrm{Gal}(K/k)$. Se $H = \mathrm{Gal}(K/M)$ per un certo campo M tale che $K \supseteq M \supseteq k$ allora $(\phi \circ \phi^{-1} \circ \phi)(M) = \phi(M) = \mathrm{Gal}(K/M) = H$. Se mostriamo che ogni sottogruppo chiuso di $\mathrm{Gal}(K/k)$ è uguale a $\mathrm{Gal}(K/M)$ per un certo campo M tale che $K \supseteq M \supseteq k$ abbiamo dunque concluso. Poiché $\mathrm{Gal}(K/k)$ è un gruppo topologico profinito allora è quasi compatto e totalmente disconnesso. Allora per la Proposizione 2.8 ogni sottoinsieme chiuso C di $\mathrm{Gal}(K/k)$ è tale che $C = \bigcap\{NC \text{ con } N \triangleleft_O G\}$ quindi C è intersezione di aperti. Supponiamo momentaneamente di aver dimostrato che ogni sottogruppo aperto di $\mathrm{Gal}(K/k)$ è uguale $\mathrm{Gal}(K/M) = \phi(M)$ per un certo campo M tale che $K \supseteq M \supseteq k$. Allora esisterebbero $A_\lambda = \mathrm{Gal}(K/M_\lambda)$ aperti di $\mathrm{Gal}(K/k)$ tali che $C = \bigcap_{\lambda \in \Lambda} A_\lambda = \bigcap_{\lambda \in \Lambda} \mathrm{Gal}(K/M_\lambda) = \mathrm{Gal}(K/S) = \phi(S)$ dove S è il più piccolo campo contenente tutti i campi M_λ, quindi avremmo concluso.
Proviamo ora che ogni sottogruppo aperto H di $\mathrm{Gal}(K/k)$ è uguale $\mathrm{Gal}(K/M) = \phi(M)$ per un certo campo M tale che $K \supseteq M \supseteq k$. Esistono una famiglia di campi $N_i \in \mathcal{F}$ e $\sigma_i \in \mathrm{Gal}(K/k)$ per ogni $i \in I$ tali che $H = \bigcup_{i \in I} \sigma_i \mathrm{Gal}(K/N_i)$. In particolare esiste $i_0 \in I$ tale che $H \supseteq \mathrm{Gal}(K/N_{i_0})$. Per semplificare le notazione poniamo $L := N_{i_0}$. Sia $S := \{\sigma_{|L} \text{ tali che } \sigma \in H\}$ che risulta essere un sottogruppo di $\mathrm{Gal}(L/k)$. Per il Teorema Fondamentale della Teoria di Galois classico si ha che esiste un campo M con $L \supseteq M \supseteq k$ tale che $S = \mathrm{Gal}(L/M)$ e quindi $L^S = M$. Proviamo che $H = \mathrm{Gal}(K/M)$. Se $\sigma \in H$ allora σ è un automorfismo di K che lascia fisso M poiché $\sigma_{|L} \in S$ lascia fisso M. Sia $\sigma \in \mathrm{Gal}(K/M)$. Dato che $L \in \mathcal{F}$ si ha che $\sigma_{|L}$ è un automorfismo di L che fissa M. Ma $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/L^S) = S$ quindi esiste $\tau \in H$ tale che $\sigma_{|L} = \tau_{|L}$. Allora per ogni $l \in L$ si ha che $(\tau^{-1} \circ \sigma)(l) = l$ quindi $\tau^{-1} \circ \sigma \in \mathrm{Gal}(K/L) \subseteq H$ quindi $\sigma \in H$.
Si verifica facilmente che se H_1 e H_2 sono due sottogruppi chiusi di $\mathrm{Gal}(K/k)$ tali che

$H_1 \subseteq H_2$ allora $\phi^{-1}(H_1) \supseteq \phi^{-1}(H_2)$.

□

Teorema 6.20. *Sia M un campo intermedio fra K e k. Nelle notazioni del Teorema 6.19 si ha che*

a) $\phi(M) = \mathrm{Gal}(K/M)$ è aperto in $\mathrm{Gal}(K/k)$ se e solo se $M \supseteq k$ è finita. In questo caso vale che $[\mathrm{Gal}(K/k) : \mathrm{Gal}(K/M)] = [M : k]$;

b) $\phi(M) = \mathrm{Gal}(K/M)$ è un sottogruppo normale di $\mathrm{Gal}(K/k)$ se e solo se $M \supseteq K$ è di Galois. In questo caso vale che $\mathrm{Gal}(M/k)$ è isomorfo come gruppo topologico a $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/M)$.

Dimostrazione. a) Se $\mathrm{Gal}(K/M)$ è aperto in $\mathrm{Gal}(K/k)$ allora esistono una famiglia di campi $F_i \in \mathcal{F}$ e $\sigma_i \in \mathrm{Gal}(K/k)$ per ogni $i \in I$, tali che $\mathrm{Gal}(K/M) = \bigcup_{i\in I} \sigma_i \mathrm{Gal}(K/F_i)$. In particolare esiste $i_0 \in I$ tale che $\mathrm{Gal}(K/M) \supseteq \mathrm{Gal}(K/F_{i_0})$. Per il Teorema 6.19 si ha che $F_{i_0} \supseteq M \supseteq k$ e dato che $F_{i_0} \supseteq k$ è finita anche $M \supseteq k$ è finita.
Se $M \supseteq k$ è finita allora esiste un $N \in \mathcal{F}$ tale che $N \supseteq M$ quindi vale che $\mathrm{Gal}(K/N) \subseteq \mathrm{Gal}(K/M)$. Dunque $\mathrm{Gal}(K/M)$ è un aperto di $\mathrm{Gal}(K/k)$.
Sia $[M : k]$ finito. Esistono $\beta_1, \ldots, \beta_m \in M \subseteq K$ tali che $M = k(\beta_1, \ldots, \beta_m)$. Poiché $\beta_1, \ldots, \beta_m \in K$ sono separabili esiste $\alpha_1 \in M$ tale che $M = k(\alpha_1)$. Se p_{α_1} è il polinomio minimo di α_1 su k si ha che $[M : k]$ è uguale al grado di p_{α_1}. Sia $\phi : M \longrightarrow K$ un omomorfismo di campi che lascia fisso k. L'omomorfismo ϕ è univocamente determinato da $\phi(\alpha_1)$ che è una radice di p_{α_1}. Ci sono dunque esattamente n di tali isomorfismi dato che p_{α_1} è separabile. Siano $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ le radici distinte di p_{α_1} e $\phi_{\alpha_1}, \phi_{\alpha_2}, \ldots, \phi_{\alpha_n}$ i relativi isomorfismi associati. Per la Proposizione 6.17 ognuno di questi isomorfismi può essere esteso ad un automorfismo in K che chiameremo rispettivamente $\tilde{\phi_{\alpha_1}}, \tilde{\phi_{\alpha_2}}, \ldots, \tilde{\phi_{\alpha_n}}$. Mostriamo che $\mathrm{Gal}(K/k) = \bigcup_{i=1}^{n} \tilde{\phi_{\alpha_i}} \mathrm{Gal}(K/M)$.
Chiaramente $\mathrm{Gal}(K/k) \supseteq \bigcup_{i=1}^{n} \tilde{\phi_{\alpha_i}} \mathrm{Gal}(K/M)$. Sia $\sigma \in \mathrm{Gal}(K/k)$ proviamo che esistono $j \in \{1, \ldots, n\}$ e $\tau \in \mathrm{Gal}(K/M)$ tali che $\sigma = \tilde{\phi_{\alpha_j}} \circ \tau$. Si ha che $\sigma_{|M}$ è univocamente determinato da $\sigma(\alpha_1) = \alpha_j$ dove $j \in \{1, \ldots, n\}$. Sia $\tau := \tilde{\phi_{\alpha_j}}^{-1} \circ \sigma$. Chiaramente τ è un automorfismo da K in K, proviamo che τ fissa M. Poiché τ fissa k basta far vedere che τ fissa α_1. Si ha che $\tau(\alpha_1) = \tilde{\phi_{\alpha_j}}^{-1} \circ \sigma(\alpha_1) = \tilde{\phi_{\alpha_j}}^{-1}(\alpha_j) = \alpha_1$. Dunque $[\mathrm{Gal}(K/k) : \mathrm{Gal}(K/M)]$ è minore o uguale a n. Se esistono $i, j \in \{1, \ldots, n\}$ tali che $\tilde{\phi_{\alpha_i}} \circ \tau_i = \tilde{\phi_{\alpha_j}} \circ \tau_j$ con $\tau_i, \tau_j \in \mathrm{Gal}(K/M)$ allora $\tilde{\phi_{\alpha_i}} \circ \tau_i(\alpha_1) = \tilde{\phi_{\alpha_i}}(\alpha_1) = \alpha_i = \alpha_j = \tilde{\phi_{\alpha_j}} \circ \tau_j(\alpha_1)$ quindi necessariamente $i = j$. Dunque $[\mathrm{Gal}(K/k) : \mathrm{Gal}(K/M)]$ è uguale a n che è uguale a $[M : k]$.

b) Supponiamo che $\mathrm{Gal}(K/M)$ sia un sottogruppo normale di $\mathrm{Gal}(K/k)$. Sia g un automorfismo di $\mathrm{Gal}(K/k)$ e $M_1 := g(M)$. Mostriamo che $\mathrm{Gal}(K/M_1)$ è uguale a $g\mathrm{Gal}(K/M)g^{-1}$. Se $\tau \in \mathrm{Gal}(K/M)$ chiaramente $g \circ \tau \circ g^{-1}$ è un automorfismo da K in K. Inoltre per ogni $g(m) \in M_1$ si ha $g \circ \tau \circ g^{-1}(g(m)) = g(m)$ poiché τ lascia fisso M. Sia $\sigma \in \mathrm{Gal}(K/M_1)$, mostriamo che $g^{-1} \circ \sigma \circ g \in \mathrm{Gal}(K/M)$. Chiaramente $g^{-1} \circ \sigma \circ g$ è un automorfismo di K e lascia fisso M poiché σ lascia fisso $g(M)$.
Per ogni $g \in \mathrm{Gal}(K/k)$ si ha che $k \subseteq g(M) \subseteq K$ e $\phi(g(M)) = \mathrm{Gal}(K/g(M)) = = g\mathrm{Gal}(K/M)g^{-1} = \mathrm{Gal}(K/M) = \phi(M)$. Allora per il Teorema 6.19 si ha che $g(M) = M$ per ogni $g \in \mathrm{Gal}(K/k)$.
Proviamo che $M \supseteq k$ è normale. Sia $p \in K[t]$ un polinomio irriducibile non costante tale che esiste $x \in M$ per cui $p(x) = 0$. Se il grado di p è uguale a uno non c'è nulla dimostrare. Sia $y \in K$ tale che $p(y) = 0$. Per il Lemma 6.18 esiste un isomorfismo $\gamma : k(x) \longrightarrow k(y)$ che fissa k e tale che $\gamma(x) = y$. Per la Proposizione 6.17 la mappa γ può essere estesa ad un automorfismo $\tilde{\gamma}$ di K. Chiaramente $\tilde{\gamma} \in \mathrm{Gal}(K/k)$, quindi $\tilde{\gamma}(M) = M$. Poiché $x_0 \in M$ si ha dunque che $\tilde{\gamma}(x_0) = y_0 \in M$.
Se $x \in M \subseteq K$ allora il suo polinomio minimo p_x su k è separabile poiché $K \supseteq k$ è separabile, quindi $M \supseteq k$ è separabile. Allora $M \supseteq k$ è una estensione di Galois.
Sia $M \supseteq k$ una estensione di campi di Galois. Analogamente a quando abbiamo definito una topologia su $\mathrm{Gal}(K/k)$ si verifica che la seguente mappa è un omomorfismo di gruppi.

$$\begin{array}{rccc} \psi : & \mathrm{Gal}(K/k) & \longrightarrow & \mathrm{Gal}(M/k) \\ & \sigma & \longmapsto & \sigma_{|M} \end{array}$$

Si ha che $\ker\psi = \mathrm{Gal}(K/M)$ quindi $\mathrm{Gal}(K/M)$ è un sottogruppo normale di $\mathrm{Gal}(K/k)$.
Inoltre ψ è una mappa suriettiva: se $\tau \in \mathrm{Gal}(M/k)$ allora per la Proposizione 6.17 la mappa τ si può estendere ad un automorfismo $\tilde{\tau}$ di K, dunque $\psi(\tilde{\tau}) = \tau$. Poiché le estensioni $K \supseteq k$ e $M \supseteq k$ sono di Galois per il Corollario 6.13 si ha che $\mathrm{Gal}(K/k)$ e $\mathrm{Gal}(M/k)$ sono gruppi topologici profiniti. Per il Teorema 2.3 si ha che $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/M)$ è isomorfo a $\mathrm{Gal}(M/k)$ come gruppo topologico.

□

Lemma 6.21. *Siano G un gruppo topologico e G' un gruppo topologico profinito. Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi e sia $\mathcal{V}$ un sistema fondamentale di intorni aperti di $1_{G'}$. Se per ogni $V \in \mathcal{V}$ si ha che $f^{-1}(V)$ è un aperto di G allora f è continua.*

Dimostrazione. Sia W un intorno aperto di $f(1_G) = 1_{G'}$ in G'. Esiste $V \in \mathcal{V}$ tale che $V \subseteq W$. Mostriamo che esiste un intorno U di 1_G in G tale che $f(U) \subseteq V$. Se poniamo $U := f^{-1}(V)$ si ha che U è un intorno aperto di 1_G tale che $f(U) = f(f^{-1}(V)) \subseteq V$. Quindi per ogni intorno aperto W di $1_{G'}$ esiste un intorno aperto di 1_G tale che $f(U) \subseteq W$. Sia $g \in G$ e sia $V_{f(g)}$ un intorno aperto di $f(g)$ in G'. Per la proposizione 2.8 si ha

che esistono una famiglia di sottogruppi aperti B_i di G' e $g'_i \in G'$ con $i \in I$ tali che $V_{f(g)} = \bigcup_{i\in I} g'_i B_i$. In particolare esiste $i_0 \in I$ tale che $f(g) \in g'_{i_0} B_{i_0} \subseteq V_{f(g)}$. Allora $f(g)B_{i_0} = g'_{i_0} B_{i_0}$. Essendo B_{i_0} un sottogruppo aperto di G' si ha che B_{i_0} è un intorno di $1_{G'}$. Quindi esiste un intorno aperto U di 1_G tale che $f(U) \subseteq B_{i_0}$. Dunque gU è un intorno aperto di g in G tale che $f(gU) = f(g)f(U) \subseteq f(g)B_{i_0} \subseteq V_{f(g)}$. Allora f è continua in ogni elememto di G.

□

Teorema 6.22. *Ogni gruppo profinito è isomorfo come gruppo topologico ad un gruppo di Galois.*

Dimostrazione. Sia G un gruppo profinito e sia F un campo arbitrario.
Consideriamo l'unione disgiunta $S := \dot{\bigcup}_{N\lhd_O G} G/N$. Sia $K := F(\{X_s \text{ tali che } s \in S\})$ con X_s trascendenti su F e algebricamente indipendenti su S. Consideriamo la seguente mappa

$$\begin{array}{rccc} \theta: & G & \longrightarrow & \mathrm{Aut}K \\ & g & \longmapsto & \psi_g : K \longrightarrow K \end{array}$$

dove ψ_g è così definita: se u è un elemento di K, $u = \sum_{\text{finita}} a_{s_1,\dots,s_r} X_{s_1}^{i_{s_1}} \cdot \ldots \cdot X_{s_r}^{i_{s_r}}$ appartenente a $F(X_{s_1}, \dots, X_{s_r})$ allora ψ_g lascia fissi i coefficenti di u e manda $X_{s_j} = X_{x_j N_j}$ in $X_{gx_jN_j} = X_{\tilde{s_j}}$ per ogni $j = 1, \dots, r$.
Per ogni $g \in G$ si ha che ψ_g è una mappa biunivoca poiché la sua mappa inversa è $\psi_{g^{-1}}$. Inoltre poiché ψ_g scambia solo gli indici delle indeterminate e lascia fissi i coefficienti degli elementi di K si ha che ψ_g è un omomorfismo di anelli.
La mappa θ è un omomorfismo di gruppi infatti per ogni $g_1, g_2 \in G$ si ha che $\theta(g_1g_2) = = \psi_{g_1g_2}$ è la mappa che manda X_{xN} in $X_{g_1g_2xN}$ che è l'immagine di X_{xN} tramite $\psi_{g_1} \circ \psi_{g_2} = \theta(g_1) \circ \theta(g_2)$.
Mostriamo che θ è iniettiva.
Se $g_1, g_2 \in G$ sono tali che $\psi_{g_1} = \psi_{g_2}$ allora per ogni $xN \in S$ si ha che $g_1xN = g_2xN$. Quindi $g_1, g_2 \in \bigcap\{N \text{ con } N\lhd_O G\}$. Poiché G è un gruppo profinito, per la Proposizione 2.8 punto c) si ha che $\bigcap\{N \text{ con } N\lhd_O G\}$ è uguale ad 1_G. Dunque $g_1 = g_2$.
Sia $u \in K$, $u = \sum_{\text{finita}} a_{s_1,\dots,s_r} X_{s_1}^{i_{s_1}} \cdot \ldots \cdot X_{s_r}^{i_{s_r}}$ con $s_i = x_iN_i$. Proviamo che

$$G_u := \{g \in G \text{ tali che } \psi_g(u) = u\}$$

contiene $N_1 \cap \ldots \cap N_r$. Se $g \in N_1 \cap \ldots \cap N_r$ allora $\psi_g(X_{s_i}) = \psi_g(X_{x_iN_i}) = X_{gx_iN_i} = = X_{x_iN_i} = X_{s_i}$. Dunque ψ_g lascia fisso X_{s_j} per ogni $j = 1, \dots, r$ e quindi lascia fisso u. Poiché $N_1 \cap \ldots \cap N_r$ è un aperto di G e G_u è un gruppo che lo contiene si ha che G_u è un aperto di G.

Consideriamo $K^{\theta(G)} = \{u \in K \text{ tali che } \theta(g)u = u \text{ per ogni } g \in G\} \subseteq K$.
Mostriamo che $K \supseteq K^{\theta(G)}$ è una estensione algebrica.
Sia $u_1 \in K$, poiché G_{u_1} è un sottogruppo aperto di G si ha che G_{u_1} ha indice finito in G per l'Osservazione 2.2 punto c). Allora esistono $g_1, \ldots, g_n \in G$ tali che $G = g_1 G_{u_1} \cup \ldots \cup g_n G_{u_1}$. Se $g \in G$ allora esistono $i \in \{1, \ldots, n\}$ e $z \in G_{u_1}$ tali che $g = g_i z$. Quindi vale che $\theta(g)u_1 = \theta(g_i z)(u_1) = \theta(g_i)(\theta(z)(u_1)) = \theta(g_i)(u_1) =: v_i$. Quindi l'insieme dei valori possibili al variare di g in G di $\theta(g)u_1$ è uguale all'insieme $\{v_1, v_2, \ldots, v_n\}$, che è uguale all'insieme $\{u_1, u_2, \ldots, u_m\}$ dove gli u_i sono gli elementi distinti di $\{v_1, v_2, \ldots, v_n\}$. Consideriamo

$$f_{u_1} := \prod_{i=1}^{m} (t - u_i) \in K[t].$$

Fissiamo $g \in G$ e consideriamo l'isomorfismo di anelli $\tilde{\theta(g)} : K[t] \longrightarrow K[t]$ definito analogamente a come è stato fatto nella Proposizione 6.2.
Si ha che

$$\tilde{\theta(g)}(f_{u_1}) = \prod_{i=1}^{m} (t - \tilde{\theta(g)}(u_i)) = \prod_{i=1}^{m} (t - \theta(g)(u_i)).$$

Al variare di i si ha che $\theta(g)u_i = \theta(gg_i)u_1$ assume m valori appartenenti a $\{u_1, \ldots, u_m\}$. Inoltre se per assurdo $\theta(g)u_i = \theta(g)u_j$ allora essendo $\theta(g)$ un automorfismo si ha che $u_i = u_j$ che è assurdo. Dunque $\tilde{\theta(g)}(f_{u_1}) = f_{u_1}$. Esistono $a_0, \ldots, a_m \in K$ tali che $f_{u_1} = a_0 + a_1 t + \ldots + a_m t^m$. Allora $\tilde{\theta(g)}(f_{u_1}) = \theta(g)(a_0) + \theta(g)(a_1)t + \ldots + \theta(g)(a_m)t^m = = a_0 + a_1 t + \ldots + a_m t^m$. Quindi $a_i = \theta(g)a_i$ per ogni $i = 1, \ldots, m$. Poiché questo ragionamento può essere ripetuto per ogni g si ha che $a_i \in K^{\theta(G)}$. Dunque $f_{u_1} \in K^{\theta(G)}[t]$ e ha come radice u_1. Quindi l'estensione $K \supseteq K^{\theta(G)}$ è algebrica.
Per ogni $u_1 \in K$ se p_{u_1} è il polinomio minimo di u_1 su $K^{\theta(G)}$ esiste $q \in K^{\theta(G)}[t]$ tale che $f_{u_1} = p_{u_1} q$. Quindi p_{u_1} è separabile. Allora l'estensione $K \supseteq K^{\theta(G)}$ è separabile.
Si ha che $K^{\theta(G)}(u_1, \ldots, u_m) \supseteq K^{\theta(G)}$ è normale. Infatti $K^{\theta(G)}(u_1, \ldots, u_m)$ è un campo di spezzamento di f_{u_1} su $K^{\theta(G)}$ e vale la Proposizione 6.3.
Ma $K \supseteq K^{\theta(G)}(u_1, \ldots, u_m) \supseteq K^{\theta(G)}$ per ogni $u_1 \in K$. Quindi si ha che

$$K = \bigcup_{u_1 \in K} K^{\theta(G)}(u_1, \ldots, u_m).$$

Dunque $K \supseteq K^{\theta(G)}$ è normale. Allora $K \supseteq K^{\theta(G)}$ è di Galois.
Chiaramente $\theta(g) \in \mathrm{Gal}(K/K^{\theta(G)})$ per ogni g.
Mostriamo che θ è continua.
Poniamo $R_{u_1} := \bigcap_{g \in G} g G_{u_1} g^{-1}$ per ogni $u_1 \in K$. Chiaramente $g G_{u_1} g^{-1}$ è un sottogruppo di G per ogni $g \in G$ e per ogni $u_1 \in K$. Quindi R_{u_1} è un sottogruppo di G per ogni $u_1 \in K$. Poiché abbiamo visto che G_{u_1} è un aperto di G, per la Proposizione 2.8 punto

a) si ha che esistono una famiglia di sottogruppi normali aperti A_j di G e $g_j \in G$ per $j \in J$ tali che $G_{u_1} = \bigcup_{j \in J} A_j g_j$. In particolare esiste $j_0 \in J$ tale che $G_{u_1} \supseteq A_{j_0}$. Poiché A_{j_0} è normale in G si ha che $A_{j_0} \subseteq g A_{j_0} g^{-1} \subseteq g G_{u_1} g^{-1}$ per ogni g, dunque $A_{j_0} \subseteq R_{u_1}$ per ogni $u_1 \in K$. Dunque R_{u_1} è un aperto di G per ogni $u_1 \in K$.
Proviamo che

$$\theta^{-1}\left(\mathrm{Gal}\left(K/K^{\theta(G)}(u_1,\ldots,u_m)\right)\right) = R_{u_1} \cap \ldots \cap R_{u_m}$$

dove $u_2, \ldots, u_m$ sono definiti come sopra. Sia $x \in G$ tale che $\theta(x)$ fissa $K^{\theta(G)}(u_1,\ldots,u_m)$. Mostriamo che per ogni $i = 1,\ldots,m$ si ha che $x \in R_{u_i}$ cioè che $g^{-1}xg \in G_{u_i}$ per ogni i e per ogni $g \in G$. Per definizione di $u_1,\ldots,u_m$ si ha che $\theta(g)(u_i) \in K^{\theta(G)}(u_1,\ldots,u_m)$, allora $\theta(x)(\theta(g)(u_i)) = \theta(g)(u_i)$ per ogni i e per ogni g. Quindi per ogni i e per ogni g si ha che $\theta(g^{-1})(\theta(x)(\theta(g)(u_i))) = u_i$. Dunque per ogni i e per ogni g si ha che $g^{-1}xg \in G_{u_i}$.
Sia $x \in R_{x_1} \cap \ldots \cap R_{x_r}$ vogliamo provare che $\theta(x)$ fissa $K^{\theta(G)}(u_1,\ldots,u_m)$. Per ogni i e per ogni g poiché $x \in g G_{u_i} g^{-1}$ si ha che $\theta(g)^{-1}\theta(x)(\theta(g)(u_i)) = u_i$. Quindi per ogni g e per ogni i si ha che $\theta(x)(\theta(g)(u_i)) = \theta(g)(u_i)$. Dunque $\theta(x)$ fissa $\theta(g)(u_i)$ per ogni i e per ogni g. Allora $\theta(x)$ fissa $u_1,\ldots u_m$. Ma $\theta(x)$ fissa anche $K^{\theta(G)}$ quindi $\theta(x)$ fissa $K^{\theta(G)}(u_1,\ldots,u_m)$.
Poiché R_{u_i} è un aperto di G per ogni i allora $\theta^{-1}\left(\mathrm{Gal}\left(K/K^{\theta(G)}(u_1,\ldots,u_m)\right)\right)$ è un aperto di G. Per il il Lemma 6.10 gli insiemi del tipo $\sigma \circ \mathrm{Gal}(K/K^{\theta(G)}(u_1,\ldots,u_m))$ con $\sigma \in \mathrm{Gal}(K/K^{\theta(G)})$ formano una base per la topologia di $\mathrm{Gal}(K/K^{\theta(G)})$. Inoltre la famiglia degli insiemi del tipo $\mathrm{Gal}\left(K/K^{\theta(G)}(u_1,\ldots,u_m)\right)$ formano chiaramente un sistema fondamentale di intorni di $1_{\mathrm{Gal}(K/K^{\theta(G)})}$. Per il Lemma 6.21 si ha che θ è continua.
Proviamo che θ suriettiva.
Poiché G è quasi compatto e θ è continua si ha che $\theta(G) \subseteq \mathrm{Gal}(K/K^{\theta(G)})$ è quasi compatto. Poiché $\mathrm{Gal}(K/K^{\theta(G)})$ è di Hausdorff si ha allora che $\theta(G)$ è chiuso. Se ϕ è la mappa definita nel teorema 6.19 si ha che $\phi^{-1}(\theta(G)) = K^{\theta(G)}$. Dunque $\theta(G) = = \phi(K^{\theta(G)}) = \mathrm{Gal}(K/K^{\theta(G)})$.
Poiché sia G che $\mathrm{Gal}(K/K^{\theta(G)})$ sono profiniti e quindi di Hausdorff e quasi compatti abbiamo che θ è un isomorfismo di gruppi topologici.

□

Esempio 9. *Esistono dei sottogruppi di gruppi di Galois di estensioni di Galois per cui non vale la corrispondenza di Galois.*

Dimostrazione. Sia $\tilde{K}$ una chiusura algebrica di $(\mathbb{Z}/p\mathbb{Z})[x] =: \mathbb{F}_p$[1]. Per ogni $n \in \mathbb{N}$ poniamo

$$\mathbb{F}_{p^n} := \{\alpha \in \tilde{K} \text{ radici di } x^{p^n} - x \in F_p[x]\}.$$

Si ha che $\mathbb{F}_{p^n}$ è un sottocampo di $\tilde{K}$ per ogni n. Chiaramente $\mathbb{F}_{P^n}$ è un campo di spezzamento di $x^{p^n} - x \in F_p[x]$. Ricordiamo che $\mathbb{F}_{p^n}$ ha caratteristica p, ha ordine p^n e

[1]Si veda ad esempio il Corollario 2.6 del libro *Algebra*, di S. Lang [5].

il grado dell'estensione $\mathbb{F}_{p^n} \supseteq \mathbb{F}_p$ è n. Essendo $x^{p^n} - x$ separabile si ha che $\mathbb{F}_{p^n} \supseteq \mathbb{F}_p$ è una estensione di Galois. Si noti che se m è un multiplo di n si ha che $\mathbb{F}_{p^n} \subseteq F_{p^m}$.
Poniamo $K := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$. Si ha che K è un sottocampo di $\tilde{K}$. Vale che $K \supseteq \mathbb{F}_p$ è una estensione di Galois poiché è unione di estensioni di Galois. Si noti che $K \supseteq \mathbb{F}_p$ ha grado infinito, infatti non può averlo finito per il Teorema della Torre.
Mostriamo che esiste un sottogruppo H di $\mathrm{Gal}(K/\mathbb{F}_p)$ per cui non vale la corrispondenza di Galois ovvero tale che $\mathrm{Gal}(K/K^H) \neq H$. Da questo segue che H è un sottogruppo di $\mathrm{Gal}(K/\mathbb{F}_p)$ che non è né chiuso né aperto. Poiché K ha come sottocampo F_p si ha che K ha caratteristica p. Dunque la seguente mappa è un automorfismo di campi.

$$\begin{array}{rccc} \phi: & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

Si ha che $\phi \in \mathrm{Gal}(K/F_p)$ poiché per ogni $\alpha \in K$ si ha che $\phi(\alpha) = \alpha$ se e solo se $\alpha^p = \alpha$ se e solo se $\alpha \in F_p$. Sia H il sottogruppo di $\mathrm{Gal}(K/F_p)$ generato da ϕ, cioè

$$H := \{\phi^k \text{ tali che } k \in \mathbb{Z}\},$$

dove se n è un intero positivo per ϕ^{-n} si intende $(\phi^{-1})^n$. Si verifica facilmente che $K^H = F_p$. Proviamo che $\mathrm{Gal}(K/K^H) \neq H$. Faremo vedere che esiste un automorfismo $\psi \in \mathrm{Gal}(K/K^H)$ tale che $\psi \notin H$.
Sia $L = \bigcup_{m=1}^{\infty} F_{p^{2^m}}$. Mostriamo che $L \neq K$. Sia ad esempio i_3 un omomorfismo di anelli da F_p a F_{p^3}. Sia $\alpha \in F_{p^3} \setminus i(F_p)$. Se si applica il Teorema della Torre alle estensioni $F_{p^3} \supseteq F_p(\alpha) \supseteq F_p$ si ha che necessariamente il grado del polinomio minimo di α su F_p deve essere 3. Proviamo che $\alpha \notin L$. Se $\beta \in L$, $\beta \in F_{p^{2^m}}$ per il Teorema della Torre il grado del polinomio minimo di β deve essere una potenza di due. Dunque $\alpha \notin L$.
Per il Teorema 6.19 si ha che $\mathrm{Gal}(K/L) \neq \mathrm{Gal}(K/K) = id_K$. Sia $\psi \in \mathrm{Gal}(K/L)$ con $\psi \neq id_K$. Chiaramente $\psi \in \mathrm{Gal}(K/F_p)$.
Poniamo per assurdo che esista un intero positivo s tale che $\psi = \phi^s$. Per il Teorema 6.19 si avrebbe che $L = K^{\mathrm{Gal}(K/L)} \subseteq \{\alpha \in K \text{ tali che } \psi(\alpha) = \alpha\}$. Se $\psi(\alpha) = \alpha$ allora $\phi^s(\alpha) = \alpha$, quindi $\alpha \in F_{p^s}$. Dunque $L \subseteq F_{p^s}$ che è assurdo poiché L ha ordine infinito, mentre F_{p^s} ha ordine finito.
Poniamo per assurdo che esista un intero positivo s tale che $\psi = \phi^{-s}$. Allora vale che $\psi^{-1} \in \mathrm{Gal}(K/F_p)$ e $\psi^{-1} = \phi^s$. Ripetendo il precedente ragionamento si ottiene un assurdo.

□

Capitolo 7

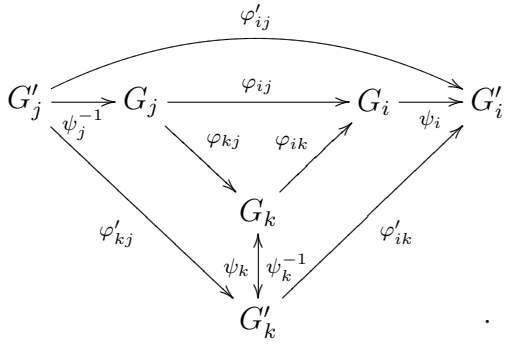
Appendice

Osservazione 7.1. *Sia (G_i, φ_{ij}) un sistema inverso di gruppi topologici indicizzato da I. Sia $G := \varprojlim G_i$. Supponiamo che esistano per ogni i dei gruppi topologici G'_i e degli isomorfismi di gruppi topologici $\psi_i : G_i \longrightarrow G'_i$. Allora*

a) (G'_i, φ'_{ij}) è un sistema inverso di gruppi topologici indicizzato da I con mappe $\varphi'_{ij} = \psi_i \circ \varphi_{ij} \circ \psi_j^{-1}$;

b) $\varprojlim G_i$ è isomorfo come gruppo topologico a $\varprojlim G'_i$.

Dimostrazione. a) Siano $i, j, k \in I$ tali che $i \leq k \leq j$. Consideriamo il seguente diagramma



.

Mostriamo che $\varphi'_{ik} \circ \varphi'_{kj} = \varphi'_{ij}$. Si ha che $\varphi'_{ik} \circ \varphi'_{kj} = \varphi'_{ij}$ se e solo se vale che $(\psi_i \circ \varphi_{ik} \circ \psi_k^{-1}) \circ (\psi_k \circ \varphi_{kj} \circ \psi_j^{-1}) = \psi_i \circ \varphi_{ij} \circ \psi_j^{-1}$ se e solo se, poiché ψ_i e ψ_j sono mappe biunivoche, si ha che $\varphi_{ik} \circ \varphi_{kj} = \varphi_{ij}$, che risulta essere vero poiché (G_i, φ_{ij}) è un sistema inverso.

b) È sufficiente dimostrare che $s \varprojlim G_i \cong s \varprojlim G'_i$. Consideriamo la seguente mappa

$$\begin{array}{rccc} \psi : & s \varprojlim G_i & \longrightarrow & s \varprojlim G'_i \\ & (h_i)_{i \in I} & \longmapsto & (\psi_i(h_i))_{i \in I}. \end{array}$$

Sia $(h_i)_i \in s\varprojlim G_i$, mostriamo che effettivamente $(\psi_i(h_i))_i \in s\varprojlim G'_i$. Si ha che $(h_k)_k \in s\varprojlim G_i$ se e solo se per ogni $i \leq j$ si ha $\varphi_{ij}(h_j) = h_i$. Ciò è vero se e solo se per ogni $i \leq j$ si ha che $\psi_i \circ \varphi_{ij} \circ (\psi_j^{-1} \circ \psi_j)(h_j) = \psi_i(h_i)$. Questo equivale ad affermare che per ogni $i \leq j$ si ha che $\varphi'_{ij} \circ p_j((\psi_k(h_k))_k) = p_i((\psi_k(h_k))_k)$, che equivale al fatto che $(\psi_k(h_k))_k \in s\varprojlim G'_i$.
Si verifica facilmente che ψ è un omomorfismo di gruppi. Si verifica facilmente anche che la seguente mappa è la mappa inversa di ψ

$$\begin{array}{rccc} \psi^{-1}: & s\varprojlim G'_i & \longrightarrow & s\varprojlim G_i \\ & (y_i)_{i\in I} & \longmapsto & (\psi_i^{-1}(y_i))_{i\in I}. \end{array}$$

Poiché le mappe ψ_i e ψ_i^{-1} sono continue per ogni i si verifica facilmente che ψ e ψ^{-1} sono continue. Dunque ψ è un isomorfismo di gruppi topologici.

□

Lemma 7.2. *Sia G un gruppo ciclico di ordine n e sia α un generatore di G. Si ha che β è un generatore di G se e solo se esiste un intero i tale che $\beta = \alpha^i$ e $(i, n) = 1$.*

Dimostrazione. Sia $\beta = \alpha^i$ con $(i, n) = 1$. Chiaramente $\beta^n = 1_G$. Sia k un intero tale che $1 \leq k < n$. Poniamo che per assurdo $(\beta)^k = 1_G$. Quindi $\alpha^{ik} = 1_G$. Poiché l'ordine di α è uguale a n allora ik sarebbe un multiplo di n. Questo è assurdo poiché $(n, i) = 1$ e $k < n$.
Sia $\beta = \alpha^i$ un generatore di G. Poniamo che per assurdo esista un primo p che divida sia i che n. Allora $\beta^{\frac{n}{p}} = (\alpha^i)^{\frac{n}{p}} = \alpha^{n\frac{i}{p}} = (\alpha^n)^{\frac{i}{p}} = 1_G$. Ma l'ordine di β è n e $\frac{n}{p} < n$, quindi abbiamo ottenuto un assurdo.

□

Esempio 10. *Sia p un primo dispari e per $r = 1, 2, \ldots$ sia $\xi_{p^r} \in \mathbb{C}$ una radice primitiva p^r-esima dell'unità. Sia $K := \mathbb{Q}(\{\xi_{p^r}$ tali che $r = 1, 2, \ldots\})$. Allora $\mathrm{Gal}(K/\mathbb{Q}(\xi_p))$ è isomorfo come gruppo topologico a $\mathbb{Z}_p$.*

Dimostrazione. Notiamo che se ξ_{p^r}, η_{p^r} sono due radici primitive p^r-esime dell'unità allora $\mathbb{Q}(\xi_{p^r}) = \mathbb{Q}(\eta_{p^r})$. Questo perché se ξ_{p^r} è una radice primitiva p^r-esima dell'unità allora le radici di $x^{p^r} - 1$ sono $\{1, \xi_{p^r}, \xi_{p^r}{}^2, \ldots, \xi_{p^r}{}^{p^r-1}\}$. Possiamo allora supporre per ogni r che $\xi_{p^r} = e^{\frac{i2\pi}{p^r}}$.
Vogliamo dimostrare che $\mathrm{Gal}(K/\mathbb{Q}(\xi_p)) \cong s\varprojlim_{r=1,2,\ldots} \mathbb{Z}/p^r\mathbb{Z}$ con mappe del sistema inverso

$$\begin{array}{rccc} \tilde{\varphi}_{ij}: & \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^i\mathbb{Z} \\ & [x]_{p^j} & \longmapsto & [x]_{p^i}. \end{array}$$

Notiamo che per ogni $k = 2, 3, \ldots$ si ha che $\xi_{p^{k-1}} = e^{\frac{i2\pi}{p^{k-1}}} = (e^{\frac{i2\pi}{p^k}})^p = \xi_{p^k}{}^p$. Dunque per ogni $k = 2, 3, \ldots$ si ha che $\xi_{p^{k-1}} \in \mathbb{Q}(\xi_{p^k})$ quindi $\mathbb{Q}(\xi_{p^k}) \supseteq \mathbb{Q}(\xi_{p^{k-1}})$.

Vogliamo utilizzare la Proposizione 6.12. Si ha che $K = \bigcup_{r=2}^{\infty} \mathbb{Q}(\xi_{p^r})$, infatti $\mathbb{Q}(\xi_p) \subseteq \mathbb{Q}(\xi_{p^2})$ e se $\alpha \in K$ esistono $r_1, \ldots, r_s \in \{1, 2, \ldots\}$ tali che $\alpha \in \mathbb{Q}(\xi_{p^{r_1}}, \ldots, \xi_{p^{r_s}}) = \mathbb{Q}(\xi_{p^{\max\{r_1,\ldots,r_s\}}})$. Per ogni $i, j \in \{2, 3, \ldots\}$ esiste $m \in \{2, 3, \ldots\}$ tale che $\mathbb{Q}(\xi_{p^m})$ contenga sia $\mathbb{Q}(\xi_{p^i})$ che $\mathbb{Q}(\xi_{p^j})$ poiché basta prendere $m = \max\{i, j\}$. Mostriamo che $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}(\xi_p)$ è di Galois. Poiché $\mathbb{Q}(\xi_{p^r})$ è il campo di spezzamento del polinomio separabile (anche se non irriducibile) $x^{p^r} - 1 \in \mathbb{Q}[x]$ su $\mathbb{Q}$ si ha che $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}$ è di Galois. Dunque per ogni $r = 2, 3, \ldots$ si ha che $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}(\xi_p)$ è di Galois. Per la proposizione 6.12 si ha che $\mathrm{Gal}(K/\mathbb{Q}(\xi_p)) \cong s\lim_{\longleftarrow r=2,3,\ldots} \mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ con mappe del sistema inverso

$$\begin{array}{rccc} \varphi_{ij}: & \mathrm{Gal}(\mathbb{Q}(\xi_{p^j})/\mathbb{Q}(\xi_p)) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\xi_{p^i})/\mathbb{Q}(\xi_p)) \\ & \sigma & \longmapsto & \sigma_{|\mathbb{Q}(\xi_{p^i})} \end{array}$$

per ogni $i \leq' j$, dove $i \leq' j$ se e solo se $\mathbb{Q}(\xi_{p^i}) \subseteq \mathbb{Q}(\xi_{p^j})$ se e solo se $i \leq j$.
Per ogni $i = 1, 2, \ldots$ si ha che l'estensione $\mathbb{Q}(\xi_{p^i}) \supseteq \mathbb{Q}$ ha grado $p^{i-1}(p-1)$ pari al grado del polinomio ciclotomico. Poiché si ha $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}(\xi_p) \supseteq \mathbb{Q}$ per il teorema della Torre si ha che il grado di $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}(\xi_p)$ è pari a p^{r-1}. Poiché $\mathbb{Q}(\xi_{p^r}) \supseteq \mathbb{Q}(\xi_p)$ è una estensione di Galois si ha che $|\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))| = p^{r-1}$.
Se mostriamo che $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ è ciclico allora esiste un isomorfismo di gruppi fra $(\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p)), \circ)$ e $(\mathbb{Z}_{p^{r-1}}, +)$.
Per ogni r è nota l'esistenza di un isomorfismo di gruppi fra il gruppo $(\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}), \circ)$ e il gruppo $((\mathbb{Z}/p^r\mathbb{Z})^*, \cdot)$. Munendo i due precedenti gruppi della topologia discreta otteniamo l'esistenza di un isomorfismo di gruppi topologici fra i due. Si ha che $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ è un sottogruppo di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q})$. Se p è un primo dispari si ha che $(\mathbb{Z}/p^r\mathbb{Z}^*, \cdot)$ è ciclico e quindi è isomorfo a $\big(\mathbb{Z}_{p^{r-1}(p-1)}, +\big)$. Allora $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ è isomorfo ad un sottogruppo di $\mathbb{Z}_{p^{r-1}(p-1)}$. Poiché i sottogruppi di $\mathbb{Z}$ sono tutti ciclici anche tutti i sottogruppi di $\mathbb{Z}_{p^{r-1}(p-1)}$ sono ciclici. Dunque per ogni $r = 2, 3 \ldots$ si ha che $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ è ciclico.
Notiamo che se σ_r è un generatore del gruppo $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ e j è un intero tale che $1 \leq j \leq r-2$, allora $\sigma_{r|\mathbb{Q}(\xi_{p^{r-j}})}$ è un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r-j}})/\mathbb{Q}(\xi_p))$. Infatti se σ_{r-j} è un generatore $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r-j}})/\mathbb{Q}(\xi_p))$ per la Proposizione 6.17 esiste $\tau_r \in \mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ tale che $\tau_{r|\mathbb{Q}(\xi_{p^{r-j}})} = \sigma_{r-j}$. Esiste un intero k tale che $\tau_r = \sigma_r{}^k$, quindi $\sigma_{r-j} = = (\sigma_r{}^k)_{|\mathbb{Q}(\xi_{p^{r-j}})} = \big(\sigma_{r|\mathbb{Q}(\xi_{p^{r-j}})}\big)^k$. Dunque $\sigma_{r|\mathbb{Q}(\xi_{p^{r-j}})}$ genera $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r-j}})/\mathbb{Q}(\xi_p))$.
Mostriamo che per ogni $r = 2, 3, \ldots$ un generatore σ_r di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ può essere esteso ad un generatore σ_{r+1} di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r+1}})/\mathbb{Q}(\xi_p))$.
Sia τ_{r+1} un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r+1}})/\mathbb{Q}(\xi_p))$. Per quanto abbiamo appena osservato $\tau_{r+1|\mathbb{Q}(\xi_{p^r})}$ è un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$. Per il Lemma 7.2 si ha che esiste un intero positivo i con $(i, p^{r-1}) = 1$ tale che $(\tau_{r+1|\mathbb{Q}(\xi_{p^r})})^i = \sigma_r$. In particolare $(i, p^r) = 1$.

Per il Lemma 7.2 si ha che $\sigma_{r+1} := {\tau_{r+1}}^i$ è un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^{r+1}})/\mathbb{Q}(\xi_p))$. Inoltre $\sigma_{r+1|\mathbb{Q}(\xi_{p^r})} = ({\tau_{r+1}}^i)_{|\mathbb{Q}(\xi_{p^r})} = (\tau_{r+1|\mathbb{Q}(\xi_{p^r})})^i = \sigma_r$.
Sia σ_2 un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^2})/\mathbb{Q}(\xi_p))$. Per ogni $r = 3, 4, \ldots$ sia σ_r un generatore di $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ tale che $\sigma_{r|\mathbb{Q}(\xi_{p^{r-1}})} = \sigma_{r-1}$. Per ogni $r = 2, 3, \ldots$ siano ψ_r gli isomorfismi di gruppi topologici da $\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p)$ in $\mathbb{Z}/p^{r-1}\mathbb{Z}$ che mandano σ_r in $[1]_{p^{r-1}}$.
Per l'Osservazione 7.1 si ha che $s\lim_{\longleftarrow r=2,3,\ldots} \mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_p))$ è isomorfo come gruppo topologico a $s\lim_{\longleftarrow r=2,3,\ldots} \mathbb{Z}/p^{r-1}\mathbb{Z}$ con mappe del sistema inverso φ'_{ij}. Per $i \leq j$

$$\begin{array}{ccccccc} & & & \overset{\varphi'_{ij}}{\frown} & & & \\ \mathbb{Z}/p^{j-1}\mathbb{Z} & \xrightarrow{\psi_j^{-1}} & \mathrm{Gal}(\mathbb{Q}(\xi_{p^j})/\mathbb{Q}(\xi_p)) & \xrightarrow{\varphi_{ij}} & \mathrm{Gal}(\mathbb{Q}(\xi_{p^i})/\mathbb{Q}(\xi_p)) & \xrightarrow{\psi_i} & \mathbb{Z}/p^{i-1}\mathbb{Z} \\ [1]_{p^{j-1}} & \longmapsto & \sigma_{j-1} & \longmapsto & \sigma_{j-1|\mathbb{Q}(\xi_{p^i})} & \longmapsto & [1]_{p^{i-1}} \end{array}$$

da cui si deduce che $\tilde{\varphi_{ij}} = \varphi'_{ij}$.

□

Lemma 7.3. *Sia l un intero maggiore o uguale a 3. Allora $5^{(2^{l-3})} \equiv 1 + 2^{l-1} \mod 2^l$.*

Dimostrazione. Proviamo la tesi per induzione su l. Se $l = 3$ allora $5^1 \equiv 1 + 2^2 \mod 2^3$. Supponiamo che $5^{(2^{l-3})} \equiv 1 + 2^{l-1} \mod 2^l$ e mostriamo che $5^{(2^{l-2})} \equiv 1 + 2^l \mod 2^{l+1}$. Esiste un intero S tale che $5^{(2^{l-3})} = 1 + 2^{l-1} + 2^l S$. Allora $\left(5^{(2^{l-3})}\right)^2 = \left(1 + 2^{l-1} + 2^l S\right)^2$. Dunque $5^{(2^{l-2})} = 1 + 2^{2(l-1)} + 2(2^{l-1}) + 2^{2l}S^2 + 2^{l+1}S(1 + 2^{l-1})$. Poiché $l \geq 3$ si ha che $2^{l+1} \leq 2^{2l-2}$. Inoltre $2^{l+1} \leq 2^{2l-2} \leq 2^{2l}$, quindi $5^{(2^{l-2})} \equiv 1 + 2^l \mod 2^{l+1}$.

□

Proposizione 7.4. *Sia l un intero maggiore o uguale a 3. Allora*

$$(\mathbb{Z}/2^l\mathbb{Z})^* = \{{[5]_{2^l}}^i \cdot {[-1]_{2^l}}^j \text{ con } i, j \in \mathbb{Z}\}.$$

Dimostrazione. Come visto nella dimostrazione del Lemma 7.3 esiste un intero T tale che $5^{(2^{l-2})} = 1 + 2^l + T2^{l+1}$, quindi $5^{(2^{l-2})} \equiv 1 \mod 2^l$. Allora l'ordine di $[5]_{2^l}$ è minore o uguale a 2^{l-2}. Poiché l'ordine di $(\mathbb{Z}/2^l\mathbb{Z})^*$ è 2^{l-1}, l'ordine di $[5]_{2^l}$ deve essere una potenza di due. Supponiamo che l'ordine di $[5]_{2^l}$ sia 2^m con $0 \leq m \leq l-2$. Per il Lemma 7.3 si ha che $[5^{(2^{l-3})}]_{2^l} = [1 + 2^{l-1}]_{2^l} \neq [1]_{2^l}$. Se $[5^{(2^{l-k})}]_{2^l} = [1]_{2^l}$ per un intero $4 \leq k \leq l$, allora $[(5^{(2^{l-k})})^{2^{k-3}}]_{2^l} = [1]_{2^l}$ che è assurdo. Quindi necessariamente l'ordine di $[5]_{2^l}$ è 2^{l-2}.
Per semplicità di notazione poniamo $A := \{{[5]_{2^l}}^i \cdot {[-1]_{2^l}}^j \text{ con } i, j \in \mathbb{Z}\}$. Chiaramente $A \subseteq (\mathbb{Z}/2^l\mathbb{Z})^*$. Mostriamo che l'ordine di A è uguale all'ordine di $(\mathbb{Z}/2^l\mathbb{Z})^*$.
Notiamo prima che per ogni $1 \leq i \leq 2^{l-2}$ si ha che $[5^i]_{2^l} \neq [-1]_{2^l}$. Se per assurdo esistesse

un intero S tale che $5^i = -1 + S2^l = -1 + (S2^{l-2})2^2$, si avrebbe che $[5^i]_4 = [-1]_4$, quindi $[2]_4 = [0]_4$ che è assurdo.
Supponiamo che esistano due coppie di interi (i,j), (r,s) con $1 \leq i, r \leq 2^{l-2}$, $1 \leq j, s \leq 2$ e $(i,j) \neq (r,s)$ tali che $[5^i]_{2^l}[(-1)^j]_{2^l} = [5^r]_{2^l}[(-1)^s]_{2^l}$. Se $i = r$ allora $[-1]_{2^l} = [1]_{2^l}$ che essendo $l \geq 3$ è assurdo. Possiamo supporre dunque che $i > r$ e $j \neq s$. Per ogni $j = 1, 2$ si ha che $[5^{i-r}]_{2^l} = [-1]_{2^l}$ che è assurdo per quanto già notato. Quindi A ha esattamente 2^{l-1} elementi. Dunque $A = (\mathbb{Z}/2^l\mathbb{Z})^*$.

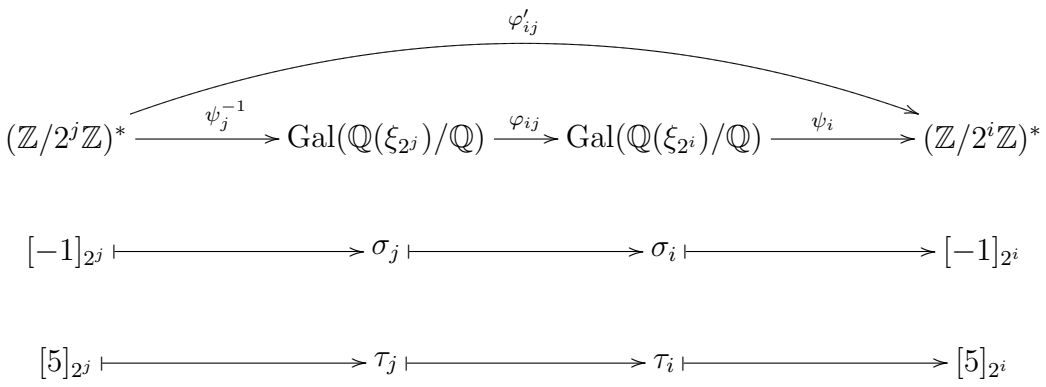
□

Esempio 11. *Sia $p = 2$ e per $r = 1, 2, \ldots$ sia $\xi_{2^r} := e^{\frac{i2\pi}{2^r}} \in \mathbb{C}$.*
Sia $K := \mathbb{Q}(\{\xi_{2^r} \text{ tali che } r = 1, 2, \ldots\})$. Allora $\mathrm{Gal}(K/\mathbb{Q}(\xi_2))$ è isomorfo come gruppo topologico a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

Dimostrazione. Analogamente all'Esempio 10 con i primi dispari, possiamo supporre per ogni $r = 1, 2, \ldots$ che $\xi_{2^r} = e^{\frac{i2\pi}{2^r}}$. Notiamo che $\xi_2 = e^{\frac{i2\pi}{2}} = -1$ quindi $\mathbb{Q}(\xi_2) = \mathbb{Q}$. Procedendo in modo analogo a quanto fatto nell'Esempio 10 si ha che $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo come gruppo topologico a $s\lim_{\longleftarrow r=3,4,\ldots} \mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q})$. Per ogni r è nota l'esistenza di un isomorfismo di gruppi ψ_r fra $(\mathrm{Gal}(\mathbb{Q}(\xi_{p^r})/\mathbb{Q})), \circ)$ e $(\mathbb{Z}/2^r\mathbb{Z}^*, \cdot)$. L'isomorfismo ψ_r manda $[l]_{2^r}$ nell'automorfismo che a ξ_{2^r} associa $\xi_{2^r}{}^l$.
Per la Proposizione 7.4 si ha che $(\mathbb{Z}/2^r\mathbb{Z})^*$ è generato da $[-1]_{2^r}$ e $[5]_{2^r}$. Quindi per ogni $r = 3, 4, \ldots$ si ha che $\mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q})$ è generato dalle mappe $\sigma_r : \xi_{2^r} \longmapsto \xi_{2^r}{}^{-1}$ e $\tau_r : \xi_{2^r} \longmapsto \xi_{2^r}{}^5$.
Siano $i, j \in \{3, 4, \ldots\}$ con $i \leq j$. Mostriamo che $\sigma_{j|\mathbb{Q}(\xi_{2^i})} = \sigma_i$. Sia $k := j - i \geq 0$. Si ha che $\sigma_{j|\mathbb{Q}(\xi_{2^i})}(\xi_{2^i}) = \sigma_{j|\mathbb{Q}(\xi_{2^i})}\left(\xi_{2^j}{}^{2^k}\right) = \sigma_j(\xi_{2^j})^{2^k} = \left(\xi_{2^j}{}^{-1}\right)^{2^k} = \left(\xi_{2^j}{}^{2^k}\right)^{-1} = \xi_{2^i}{}^{-1} = \sigma_i(\xi_{2^i})$.
Analogamente si ha che $\tau_{j|\mathbb{Q}(\xi_{2^i})} = \tau_i$.
Dunque $s\lim_{\longleftarrow r=3,4,\ldots} \mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q})$ è isomorfo come gruppo topologico a

$$s\lim_{\longleftarrow r=3,4,\ldots} (\mathbb{Z}/2^r\mathbb{Z})^*$$

avente le seguenti mappe del sistema inverso



Per ogni $r = 3, 4, \ldots$ si ha che $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ è generato da $([1]_2, [0]_{2^{r-2}})$ e $([0]_2, [1]_{2^{r-2}})$.
Per ogni $r = 3, 4, \ldots$ siano ψ_r gli isomorfismi di gruppi topologici fra $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ e $(\mathbb{Z}/2^r\mathbb{Z})^*$ che mandano $([1]_2, [0]_{2^{r-2}})$ in $[-1]_{2^r}$ e mandano $([0]_2, [1]_{2^{r-2}})$ in $[5]_{2^j}$.
Si ottiene dunque che $s\lim\limits_{\longleftarrow r=3,4,\ldots} \mathrm{Gal}(\mathbb{Q}(\xi_{2^r})/\mathbb{Q}) \cong s\lim\limits_{\longleftarrow r=3,4,\ldots} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z})$ con mappe del limite inverso

$$\begin{array}{rccc} \varphi_{ij}: & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^j\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^i\mathbb{Z} \\ & ([x]_2, [y]_{2^j}) & \longmapsto & ([x]_2, [y]_{2^i}). \end{array}$$

Quindi si ha che $s\lim\limits_{\longleftarrow r=3,4,\ldots} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z})$ è uguale a

$$\{([x_k]_2, [y_k]_{2^k}) \in \prod_{k=1}^{\infty} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}) \text{ tale che } ([x_j]_2, [y_j]_{2^i}) = ([x_i]_2, [y_i]_{2^i}) \text{ per ogni } i \leq j\}.$$

Si ha dunque che la seguente mappa è un isomorfismo di gruppi topologici

$$\begin{array}{rccc} f: & s\lim\limits_{\longleftarrow r=3,4,\ldots} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times s\lim\limits_{\longleftarrow r=3,4,\ldots} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}) \\ & \big([x_{r-2}]_2, [y_{r-2}]_{2^{r-2}}\big)_{r=3,4,\ldots} & \longmapsto & \big([x_{r-2}]_2, ([y_{r-2}]_{2^{r-2}})_{r=3,4,\ldots}\big). \end{array}$$

□

Ringraziamenti

Vorrei poter ringraziare alcune persone che in questi anni mi sono state di aiuto per il raggiungimento di questo risultato. Ringrazio Elena Meucci, compagna di studio eccezionale, per avermi fatto intravedere una possibile vita migliore. Ringrazio mia madre, i membri della mia famiglia e gli amici che mi sono stati vicini. Chiedo scusa a chi fra questi ho fatto stare troppo in ansia.
Ringrazio la professoressa Marta Morigi per avermi sup (ma anche sop, e so che non sempre deve essere stato facile) portato sia in questa che nella precedente tesi di laurea. Ringrazio anche la professoressa Mirella Manaresi, per la sua grinta, e la professoressa Monica Idà, da cui ho imparato molto, che ancora oggi mi salutano. Ringrazio la dottoressa Alessia Kogoj per una pacca sulla spalla data in tempi più difficili di questi.

Bibliografia

[1] M. Cornalba, dispense. *http://www-dimat.unipv.it/cornalba/dispense*.

[2] D. A. Cox, *Galois Theory*, John Wiley and Sons, New Jersey, 2004.

[3] S. Gabelli, *Teoria delle equazioni e teoria di Galois* , Springer, Milano, 2008.

[4] P.J. Higgins, *An Introduction to Topological Groups*, Cambridge University Press, Cambridge, 1974.

[5] S. Lang, *Algebra*, Springer, New York, 2002.

[6] L. Ribes, P. Zalesskii, *Profinite Groups*, Springer, Berlin, 2000.

[7] A. Vistoli, *Note di Algebra*.

[8] J.S. Wilson, *Profinite Groups*, Oxford University Press Inc., New York, 1998.