UNIVERSITÀ DEGLI STUDI DI TRENTO

DIPARTIMENTO DI MATEMATICA

Corso di Laurea in Matematica

Tesi di laurea

Corrispondenza di Galois per estensioni di grado infinito

Relatore
Andrea Caranti

Candidato
Giovanni Tognolini

Anno Accademico 2017–2018

Indice

Introduzione

Questo lavoro nasce come proseguimento del corso di Teoria di Galois, che ho seguito nell'A.A.2017/18. Durante il corso abbiamo avuto modo di conoscere e vedere applicato il teorema fondamentale della teoria di Galois, il quale, data un'estensione di Galois di grado finito, stabilisce una biiezione fra il reticolo dei campi intermedi e il reticolo dei sottogruppi del gruppo di Galois associato. Lo scopo di questo lavoro è di trattare un classico approccio costruttivo che estende il teorema fondamentale al caso delle estensioni di Galois di grado arbitrario. Si vedrà subito come non sia possibile in generale stabilire una corrispondenza che comprenda tutti i sottogruppi intermedi. Porremmo rimedio a tale problema seguendo un'idea di Krull, dotando cioè il gruppo di Galois di una particolare topologia, detta appunto la topologia di Krull, che lo rende un gruppo topologico; risulterà allora che vi è una biiezione fra i sottogruppi chiusi in tale topologia e i campi intermedi.

Il primo capitolo è dedicato ad alcune definizioni e risultati di base riguardo la teoria dei campi e la teoria di Galois per estensioni di grado finito. Segue poi un capitolo sui gruppi topologici, mentre nel terzo capitolo discuteremo la costruzione dei limiti inversi, andando a considerare in particolare i limiti inversi di famiglie di gruppi finiti; mostreremo che tali oggetti sono a loro volta gruppi, e andremo a dotarli di una particolare topologia, così da poterli considerare come gruppi topologici. Le strutture così ottenute prendono il nome di gruppi profiniti, e si presentano naturalmente nella trattazione delle estensioni di Galois in dimensione infinita. A fine capitolo introduciamo la topologia di Krull, che permetterà come detto di estendere al caso infinito il teorema fondamentale. Infine, l'argomento principale dell'ultimo capitolo è il teorema di corrispondenza per le estensioni infinite, in cui abbiamo rimarcato il confronto con il caso finito. Il capitolo si chiude con alcune considerazioni sulle estensioni di Galois in dimensione infinita, mostrando come sia facile incontrarle nello studio della teoria dei campi, e confermando quindi l'utilità del teorema fondamentale nella sua forma più generale.

Capitolo 1

Estensioni di Galois: risultati elementari

Enunciamo dapprima alcune definizioni e risultati importanti riguardo le estensioni di campi; questi concetti costituiranno un prerequisito essenziale per poter caratterizzare le estensioni di Galois, sia in dimensione finita che in dimensione infinita.

1.1 Estensioni e chiusure algebriche

Ricordiamo brevemente che un campo E si dice algebricamente chiuso se ogni polinomio a coefficienti in E ammette almeno una radice in E. Un'estensione di campi E/F si dice algebrica se ogni $\alpha \in E$ è algebrico su F, ovvero esiste $f \in F[Y] \setminus \{0\}$ tale che $f(\alpha) = 0$. Infine un'estensione di campi E/F si dice chiusura algebrica di F se è algebrica ed E è algebricamente chiuso.

Enunciamo ora alcuni risultati elementari molto utili, di cui faremo uso in seguito.

Lemma 1.1. *Un campo E è algebricamente chiuso se e solo se non ha estensioni proprie di grado finito.*

Lemma 1.2. *Se E è una estensione algebrica di F allora $|E| \leq \aleph_0|F|$.*

Lemma 1.3. *Sia $F \subseteq E$ una estensione di campi e sia M un campo intermedio. Se M è algebrica su F ed E è algebrica su M allora E è algebrica su F.*

Teorema 1.4. *Ogni campo ammette una chiusura algebrica.*

Dimostrazione. Sia k un campo, allora possiamo considerare un insieme S per cui valga $\aleph_0|k| < |S|$. Poiché vale sempre la relazione $|k| \leq \aleph_0|k|$ otteniamo che esiste una mappa iniettiva $f : k \to S$ e possiamo pertanto considerare k come un sottoinsieme di S. Consideriamo ora la famiglia

$$\mathcal{F} := \{(E, +, \cdot) \mid k \subseteq E \subseteq S,\ (E, +, \cdot) \text{ campo},\ E/k \text{ algebrica}\}$$

Introduciamo ora una relazione $R \subseteq \mathcal{F} \times \mathcal{F}$ definita da

$$R := \{((E, +_E, \cdot_E), (F, +_F, \cdot_F)) \in \mathcal{F} \times \mathcal{F} : E \subseteq F \text{ e } (+_E)_{|_F} = +_F\}$$

Osserviamo che:

- $(\mathcal{F}, R) \neq \emptyset$ infatti $(k, +, \cdot) \in \mathcal{F}$;
- $(\mathcal{F}, R)$ è parzialmente ordinato ovviamente;
- $\mathcal{F}$ è induttivo: sia $\mathcal{C} \subseteq \mathcal{F}$ una catena, allora un maggiorante di $\mathcal{C}$ in $\mathcal{F}$ è dato da $\bigcup \mathcal{C}$, infatti ovviamente $\bigcup \mathcal{C}$ è un maggiorante, dal momento che $C \in \bigcup \mathcal{C}$ per ogni $C \in \mathcal{C}$; mostriamo che appartiene a $\mathcal{F}$.
  Siano $a, b \in \bigcup \mathcal{C}$, allora $a \in E_1, b \in E_2$ per certi $E_1, E_2 \in \mathcal{C}$, e possiamo supporre, senza perdita di generalità, che $E_1 \subseteq E_2$; definiamo quindi $a + b := a +_{E_2} b$ e $a \cdot b := a \cdot_{E_2} b$. Si verifica facilmente che tali operazioni sono ben definite e che E è un campo.
  Sia $a \in \bigcup \mathcal{C}$ un elemento qualsiasi, allora $a \in E$, per qualche $E \in \mathcal{C}$; essendo E algebrico su k, si ottiene a algebrico, e quindi tutta l'estensione $\bigcup \mathcal{C}$ è algebrica su k.

Sono soddisfatte le ipotesi del lemma di Zorn, pertanto l'insieme $(\mathcal{F}, R)$ ammette almeno un elemento massimale $(A, +, \cdot)$. Mostriamo che A è una chiusura algebrica di k. Essendo $k \subseteq A$ un'estensione algebrica è sufficiente dimostrare che A è algebricamente chiuso ossia, per quanto detto con il Lemma 1.1, che non ha estensioni proprie di grado finito. Se per assurdo esistesse $k \subseteq A \subseteq B$ di grado finito, allora, per il Lemma 1.3, B è algebrico su k. Se k è infinito, per il Lemma 1.2, $|B| \leq \aleph_0 |k| = |k|$, se invece è finito otteniamo $|B| \leq \aleph_0 |k| = \aleph_0$. In entrambi i casi $|B| \leq |S|$ e quindi possiamo costruire una mappa iniettiva $f : B \to S$ tale che $f_{|_A} = id_A$. Indichiamo con $B' := im(f)$, allora B' ha una naturale struttura di campo indotta da quella di B tramite f, e pertanto $B' \in \mathcal{F}$, e questo contraddice la massimalità di $(A, +, \cdot)$ in $\mathcal{F}$, il che è assurdo. □

1.2 Separabilità e normalità

In questa sezione riassumiamo brevemente le proprietà caratterizzanti sia delle estensioni normali, che di quelle separabili, mostrando la stretta connessione di queste con una generica estensione di Galois. Precisiamo innanzitutto la definizione che utilizzeremo di estensione di Galois.

Definizione 1.5. Sia E/F un'estensione di campi. Denotiamo con

$$\mathrm{Gal}(E/F) := \{f : E \to E \text{ automorfismi} \mid f_{|F} = id_F\}.$$

L'estensione E/F è detta di Galois se

$$E^{\mathrm{Gal}(E/F)} := \{\alpha \in E : f(\alpha) = \alpha \ \forall f \in \mathrm{Gal}(E/F)\} = F.$$

Definizione 1.6. Sia E/F un'estensione di campi. E/F si dice separabile se il polinomio minimo su F di ogni elemento di E ha radici distinte nel suo campo di spezzamento. E/F si dice normale se il polinomio minimo su F di ogni elemento di E ha tutte le sue radici in E, equivalentemente se ogni polinomio irriducibile in $F[Y]$ che ha una radice in E ha tutte le sue radici in E.

Andiamo ora ad enunciare e dimostrare il teorema dell'elemento primitivo, un risultato della teoria dei campi che caratterizza le estensioni algebriche semplici, ovvero che possono essere generate da un unico elemento.

Teorema 1.7 (elemento primitivo)**.** *Sia $E := F(\alpha_1, ..., \alpha_n)$ un'estensione finita di campi, e supponiamo $\alpha_1, ..., \alpha_n$ separabili su F. Allora esiste un elemento $\alpha \in E$ tale che α è separabile su F e tale che valga $E = F(\alpha)$. Inoltre, se F è infinito, esistono $t_1, ..., t_n \in F$ tali che $\alpha = \alpha_1 t_1 + \cdots + \alpha_n t_n$.*

Dimostrazione. Distinguiamo separatamente i casi:

- F campo infinito:
  Dimostriamo per induzione su n che esistono $t_1, ..., t_n \in F$ tali che $\alpha := \alpha_1 t_1 + \cdots \alpha_n t_n$ è separabile su F ed $E = F(\alpha)$.
  Consideriamo dapprima il caso $n = 2$. Supponiamo $E = F(\beta, \gamma)$, con β, γ separabili su F. Sia $f \in F[Y]$ il polinomio minimo di β su F, poniamo $l := \deg(f)$ e sia $\{\beta =: \beta_1, ..., \beta_l\}$ l'insieme delle sue radici; analogamente sia $g \in F[Y]$ il polinomio minimo di γ su F, poniamo $m := \deg(g)$ e $\{\gamma =: \gamma_1, ..., \gamma_m\}$ le sue radici.
  Claim: esiste $\lambda \in F$ tale che $\beta_i \neq \beta + \lambda\gamma - \lambda\gamma_j$ per ogni $i \in \{1, ..., l\}$ e $j \in \{2, ..., m\}$.
  Consideriamo l'insieme
  $$\left\{ \frac{\beta_i - \beta_r}{\gamma_s - \gamma_j} \right\}_{i,r,s,j}$$
  al variare di $1 \leq r, i \leq l$ e $1 \leq s, j \leq m$, con $s \neq j$. Questo insieme è composto da un numero finito di elementi, ma per ipotesi F è infinito, pertanto esiste $\lambda \in F$ tale che $\lambda \neq \frac{\beta_i - \beta_r}{\gamma_s - \gamma_j}$, comunque scelti i, r, s, j come sopra. Segue che
  $$\begin{aligned} \lambda(\gamma_s - \gamma_j) &\neq \beta_i - \beta_r, \\ \lambda\gamma_s - \lambda\gamma_j &\neq \beta_i - \beta_r, \\ \lambda\gamma_s + \beta_r &\neq \lambda\gamma_j + \beta_i. \end{aligned}$$
  In particolare, ponendo $\beta_r = \beta$ e $\gamma_i = \gamma$ allora $\forall i \in \{1, ..., l\}$ e $\forall j \in \{2, .., m\}$ vale $\beta_i \neq \beta + \lambda\gamma - \lambda\gamma_j$, come richiesto.
  Claim: $F(\beta + \lambda\gamma) = F(\beta, \gamma)$.

  - $\subseteq$ Ovviamente: $\lambda \in F$ e $\beta, \gamma \in F(\beta, \gamma)$, pertanto $\beta + \lambda\gamma \in F(\beta, \gamma)$.
  - $\supseteq$ Proviamo che $\beta, \gamma \in F(\beta + \lambda\gamma)$; mostriamo dapprima che $\gamma \in F(\beta + \lambda\gamma)$.
    Osserviamo che $g(Y) \in F[Y] \subseteq F(\beta + \lambda\gamma)[Y]$ si annulla per $Y = \gamma$, così come $f(\beta + \lambda\gamma - \lambda Y) \in F(\beta + \lambda\gamma)[Y]$ si annulla per $Y = \gamma$. Consideriamo $h := gcd(g(Y), f(\beta + \lambda\gamma - \lambda Y))$ e proviamo che h è un polinomio di grado 1. Sicuramente $h \neq 1$, infatti se per assurdo così non fosse, allora esisterebbero $A(Y), B(Y) \in F(\beta + \lambda\gamma)[Y]$ tali che
    $$A(Y)g(Y) + B(Y)f(\beta + \lambda\gamma - \lambda Y) = 1.$$
    Allora per $Y = \gamma$ avremmo $0+0 = 1$, il che è assurdo. Il ragionamento è analogo per ogni costante $c \neq 0$. Abbiamo in questo modo provato che $deg(h) \neq 0$. Se per assurdo fosse $deg(h) > 1$, poiché g è separabile avremmo che, nel suo campo di spezzamento
    $$g(Y) = (Y - \gamma)(Y - \gamma_2) \cdots (Y - \gamma_m).$$
    Quindi $h(Y)$ è un polinomio della forma
    $$h(Y) := \prod_{k=1}^{r} (Y - \gamma_{i_k})$$

per qualche $r \geq 2$. Esiste quindi $j \in \{2, ..., m\}$ tale che $h(\gamma_j) = 0$, di conseguenza, poiché $h(Y)|f(\beta + \lambda\gamma - \lambda Y)$, si avrebbe che $\beta + \lambda\gamma - \lambda\gamma_j$ è radice di f, in particolare, poiché abbiamo già indicizzato tutte le radici di f, otteniamo

$$\beta_i = \beta + \lambda\gamma - \lambda\gamma_j$$

Ma questo è assurdo, per quanto mostrato prima. Concludiamo quindi che $h(Y) = Y - \gamma \in F(\beta + \lambda\gamma)[Y]$, ovvero $\gamma \in F(\beta + \lambda\gamma)$. Mostrare ora che $\beta \in F(\beta + \lambda\gamma)$ è immediato, dal momento che $\beta = (\beta + \lambda\gamma) - \lambda\gamma \in F(\beta + \lambda\gamma)$.

Claim: $\beta + \lambda\gamma$ è separabile su F.
Sia $p(Y) \in F[Y]$ il polinomio minimo di $\beta+\lambda\gamma$ su F. Considero il polinomio ausiliario

$$s(Y) := \prod_{j=1}^{m} f(Y - \lambda\gamma_j).$$

Proveremo che $\beta + \lambda\gamma$ è radice di s, $s(Y) \in F[Y]$, $p|s$ in $F[Y]$ e che s ha tutte le radici distinte; da ciò seguirà che p è separabile.

1. Mostriamo innanzitutto che $\beta + \lambda\gamma$ è radice di s:
$$\begin{aligned} s(\beta + \lambda\gamma) &= \prod_{j=1}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) \\ &= f(\beta + \lambda\gamma - \lambda\gamma) \prod_{j=2}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) \\ &= f(\beta) \prod_{j=2}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) \\ &= 0. \end{aligned}$$
2. Consideriamo il polinomio $S(Y) := \prod_{j=1}^{m} f(Y - \lambda Y_j)$. Ricordiamo che un corollario del teorema di Newton per polinomi simmetrici afferma che se $f(Y_1, ..., Y_n)$ è un polinomio simmetrico a coefficienti in un campo F, e g è un polinomio a coefficienti in F di grado n, con radici $\{\gamma_1, ..., \gamma_n\}$, allora $f(\gamma_1, ..., \gamma_n) \in F$.
Osserviamo che $S(Y)$ ha come coefficienti dei polinomi simmetrici in $Y_1, ..., Y_m$, e poiché $\{\gamma_1, ..., \gamma_m\}$ sono le radici di g, che è un polinomio in $F[Y]$ di grado m, allora i coefficienti di S, valutati in $\gamma_1, ..., \gamma_m$, hanno valore in F. Si ha quindi che
$$s(Y) = \prod_{j=1}^{m} f(Y - \lambda\gamma_j) \in F[Y].$$
3. Risulta chiaro che $\beta + \lambda\gamma$ è radice sia di p che di f, pertanto $p|s$ in $F[Y]$.
4. Proviamo che s ha radici tutte distinte
$$\begin{aligned} s(Y) &= \prod_{j=1}^{m} f(Y - \lambda\gamma_j) \\ &= \prod_{j=1}^{m} \prod_{i=1}^{l} ((Y - \lambda\gamma_j) - \beta_i) \\ &= \prod_{j=1}^{m} \prod_{i=1}^{l} (Y - (\lambda\gamma_j + \beta_i)). \end{aligned}$$

Per quanto visto all'inizio possiamo quindi affermare che le radici di s , e quindi le radici di p, sono tutte distinte. Dunque p è separabile, inoltre, ponendo $t_1 = 1$ e $t_2 = \lambda$ abbiamo provato l'enunciato per $n = 2$.
Consideriamo quindi il caso generico $n > 2$. Sia $E := F(\alpha_1, ..., \alpha_n)$. Chiaramente $F \subseteq F(\alpha_1, ..., \alpha_{n-1}) \subseteq F(\alpha_1, ..., \alpha_n)$ e per ipotesi induttiva esistono $t_1, ..., t_{n-1} \in F$ tali che $\alpha_0 := t_1\alpha_1 + \cdots t_n\alpha_{n-1}$ è separabile e primitivo, ovvero $F(\alpha_1, ..., \alpha_{n-1}) = F(\alpha_0)$. Ora $F(\alpha_1, ..., \alpha_n) = F(\alpha_0, \alpha_1)$, quindi esistono $\tilde{t_0}, \tilde{t_1} \in F :\ \alpha := \tilde{t_0}\alpha_0 + \tilde{t_1}\alpha_1$ sia separabile e primitivo, ovvero $F(\alpha_1, ..., \alpha_n) = F(\alpha)$.

- F campo finito:
  Ricordiamo che se F è un campo e $A \subseteq F^\times$ è un sottogruppo finito del gruppo moltiplicativo di F, allora A è ciclico. Sia quindi F un campo finito; per ipotesi $[\,E : F\,] < \infty$, pertanto E è un campo finito ed $E^\times$ è un gruppo ciclico, ovvero $E^\times = (\alpha)$ per qualche $\alpha \in E$. Proviamo che $E = F(\alpha)$. Ovviamente $F(\alpha) \subseteq E$, viceversa, poiché $E = E^\times \cup \{0\}$, e $F(\alpha)$ contiene sia $\{0\}$ che tutte le potenze di α, ricaviamo immediatamente $F(\alpha) \supseteq E^\times \cup \{0\} = E$, da cui l'asserto. Mostriamo ora che α è separabile su F. Sia $m := |E^\times|$, allora $\alpha^m = 1$, inoltre α^i è radice di $f := Y^m - 1$ per ogni $i \in \{0, ...m-1\}$. Poniamo $f = (Y-\alpha^0)(Y-\alpha^1)\cdots(Y-\alpha^{m-1})$, allora $f \in F[Y]$ è separabile, e pertanto anche α lo è.

□

Corollario 1.8. *Sia E/F un'estensione algebrica separabile finita. Allora esiste un elemento $\alpha \in E$ primitivo, ovvero tale che $E = F(\alpha)$.*

La definizione che abbiamo dato di un' estensione di Galois non è molto operativa. Nelle righe seguenti daremo quindi una caratterizzazione più maneggevole di un'estensione di Galois finita, facendo uso dei risultati mostrati finora. Avremo in ogni caso bisogno di due lemmi d'appoggio.

Lemma 1.9. *Sia F un campo e sia f un polinomio separabile in $F[Y]$. Sia E un campo di spezzamento di f su F. Allora $|Gal(E/F)| = |E : F|$.*

Lemma 1.10. *Sia E/F un'estensione di campi e supponiamo che il grado $[\,E : F\,]$ sia finito. Allora E/F è un'estensione di Galois se e solo se $|E : F| = |Gal(E/F)|$.*

Proposizione 1.11. *Sia E/F un'estensione finita di campi. Sono equivalenti*

1 E/F è di Galois;

2 E/F è un'estensione normale e separabile;

3 E è il campo di spezzamento di un polinomio separabile a coefficienti in F.

Dimostrazione.

$1 \Rightarrow 2$ Supponiamo E/F di Galois e poniamo $G := \mathrm{Gal}(E/F)$.
Sia $\alpha \in E$ e sia $f \in F[Y]$ il suo polinomio minimo. Consideriamo l'insieme $\{\sigma(\alpha)\}_{\sigma \in G}$; si verifica facilmente che $\sigma(\alpha) \in \mathrm{root}(f)$ per ogni $\sigma \in$ G e che pertanto l'insieme di cui sopra è finito. Possiamo pertanto indicare con $\alpha_1, ..., \alpha_r$ gli elementi distinti di $\{\sigma(\alpha)\}_\sigma$ e considerare il polinomio

$$q := (Y - \alpha_1)\cdots(Y - \alpha_r) \in E[Y].$$

Per ogni $\sigma \in G$ consideriamo la mappa

$$\begin{aligned} \tilde{\sigma}: \qquad E[Y] &\longrightarrow E[Y] \\ a_n x^n + ... + a_0 &\longmapsto \sigma(a_n)x^n + ... + \sigma(a_0). \end{aligned}$$

Si verifica facilmente che $\tilde{\sigma}$ è un automorfismo di $E[Y]$. D'altra parte si ha $\tilde{\sigma}(q) = (Y - \sigma(\alpha_1)) \cdots (Y - \sigma(\alpha_r)) = (Y - \alpha_1) \cdots (Y - \alpha_r) = q$ e pertanto, se $q = Y^r + a_{r-1}Y^{r-1} + \cdots + a_0$, allora $\sigma(a_i) = a_i$ per ogni $\sigma \in G$. Segue che $a_i \in E^G = F$ e quindi $q \in F[Y]$. Ma allora, poiché $q(\alpha) = 0$, e f è il polinomio minimo di α su F si ha che $f|q$. Di conseguenza f ha tutte le radici in E ed è separabile, quindi E/F è un'estensione normale e separabile.

$2 \Rightarrow 3$ Per ipotesi E/F è un'estensione finita, quindi esistono $\alpha_1, ..., \alpha_s \in E$ con $E = F(\alpha_1, ..., \alpha_s)$. Sia $p_i \in F[Y]$ il polinomio minimo di α_i. Allora ogni polinomio p_i è separabile e, di conseguenza, è separabile anche il polinomio $f := p_1 \cdots p_s$. Essendo E/F un'estensione normale, segue che ogni p_i si decompone completamente su E e quindi E è il campo di spezzamento di f su F .

$3 \Rightarrow 1$ Per ipotesi E è il campo di spezzamento di un polinomio separabile $f \in F[Y]$. Dal Lemma 1.9 segue che $|\mathrm{Gal}(E/F)| = |E : F|$. Quindi E/F è un'estensione di Galois per il Lemma 1.10.

□

Questo conclude la caratterizzazione delle estensioni di Galois di grado finito, tuttavia vorremmo poter descrivere in modo più operativo anche una generica estensione di Galois di dimensione infinita. I risultati che seguono vengono incontro proprio a questa esigenza.

Lemma 1.12. *(Lemma di Zorn). Sia (A, R) un insieme parzialmente ordinato, non vuoto ed induttivo, allora A ammette almeno un elemento massimale.*

Il lemma di Zorn è equivalente all'assioma della scelta e al teorema del buon ordinamento, ma la sua peculiare formulazione risulta di maggior utilità in moltissime dimostrazioni; vediamone subito un'applicazione.

Lemma 1.13. *Sia K/k un'estensione algebrica, normale e separabile, e sia $k \subseteq L \subseteq K$. Allora ogni k-morfismo $\varphi : L \to K$ si può estendere ad un automorfismo di K.*

Dimostrazione. Consideriamo l'insieme

$$\mathcal{F} := \{(F, \psi) | L \subseteq F \subseteq K, \psi : F \to \overline{K} \text{ tale che } \psi_L = \varphi\},$$

e poniamo su $\mathcal{F}$ una relazione binaria R definita da

$$(F, \psi)\, R\, (G, \omega) \Leftrightarrow F \subseteq G \text{ e } \omega_{|_F} = \psi.$$

Osserviamo che

- $\mathcal{F} \neq \emptyset$, dal momento che $(L, \varphi) \in \mathcal{F}$;
- $(\mathcal{F}, R)$ è parzialmente ordinato;
- $(\mathcal{F}, R)$ è induttivo: sia $\mathcal{C} := (F_i, \psi_i)_{i \in I} \subseteq \mathcal{F}$ una catena, allora $(F, \psi) := (\bigcup_i F_i, \bigcup_i \psi_i)$ è un maggiorante di $\mathcal{C}$ in $\mathcal{F}$.

Abbiamo quindi che $(\mathcal{F}, R)$ soddisfa le ipotesi del lemma di Zorn; sia allora (M, ψ) un elemento massimale e proviamo che $M = K$. Se per assurdo $M \subsetneq K$, sia $\alpha \in K \setminus M$ e mostriamo che è possibile estendere ψ ad un k-morfismo di $M(\alpha)$ in $\overline{K}$. Poiché l'estensione K/k è algebrica, anche K/M lo è, ed esiste f polinomio minimo di α su M. L'estensione K/k è di normale e separabile, pertanto f ha tutte le sue radici in K, e queste radici sono distinte. Consideriamo ora la mappa

$$\begin{aligned} \psi^*: \qquad M[Y] &\longrightarrow \psi(M)[Y] \\ a_nY^n + \cdots + a_0 &\longmapsto \psi(a_n)Y^n + \cdots + \psi(a_0). \end{aligned}$$

e osserviamo che $f^* := \psi^*(f)$ è irriducibile in $\psi(M)[Y]$, essendo ψ^* isomorfismo. Segue che f^* non può avere nessuna radice in $\psi(M)$, infatti se $\beta \in \psi(M)$ fosse una radice di f^*, allora esisterebbe $g \in \psi(M)[Y]$ tale che $f^* = (x - \beta)g$, e questo violerebbe l'irriducibilità di f^*. Sia quindi $\beta \in \overline{K} \setminus \psi(M)$ una radice di f^*.
Allora f^* è il polinomio minimo di β su $\psi(M)$, e pertanto l'insieme $\{1, \beta, \beta^2, ..., \beta^{deg(f)-1}\}$ costituisce una base di $\psi(M)(\beta)$ su $\psi(M)$. Definiamo ora la mappa

$$\begin{aligned} w: \qquad M(\alpha) &\longrightarrow \overline{K} \\ a_n\alpha^n + ... + a_0 &\longmapsto \psi(a_n)\beta^n + ... + \psi(a_0). \end{aligned}$$

Si verifica immediatamente che w che è un k-morfismo di $M(\alpha)$ che estende ψ.
Siamo riusciti ad estendere (M, ψ), contraddicendo la sua massimalità; necessariamente $M = K$. In questo modo abbiamo mostrato che ψ è un morfismo di K in $\overline{K}$, ma ψ è chiaramente iniettivo, essendo un morfismo di campi diverso dal morfismo nullo, mostriamo pertanto che $\psi(K) = K$.

- $\supseteq$ Sia $\gamma \in K$ e sia f il polinomio minimo di γ su k. Osserviamo che ψ manda radici di f in radici di f, infatti $f(\psi(\gamma)) = a_n(\psi(\gamma))^n + ... + a_0 = \psi(a_n\gamma^n) + ... + a_0 = \psi(a_n\gamma^n + ... + a_0) = 0$, pertanto, essendo ψ iniettiva, induce una biiezione sull'insieme $\{\gamma = \gamma_1, ..., \gamma_s\}$ delle radici di f. In particolare esiste $\gamma_i \in K$ tale che $\psi(\gamma_i) = \gamma$.

- $\subseteq$ Sia $\gamma \in \psi(K)$, allora $\gamma = \psi(\alpha)$ per qualche $\alpha \in K$. Poniamo f il polinomio minimo di α su k, allora ψ mappa radici di f in radici di f, che sono elementi di K, per la normalità assunta di K.

□

Con la teoria mostrata fin qua possiamo caratterizzare un'estensione di Galois, anche di grado infinito, così come specificato nella seguente proposizione.

Proposizione 1.14. *Sia E/F un'estensione di algebrica di campi. E/F è di Galois se e solo se è normale e separabile.*

Dimostrazione.

- $\Rightarrow$ Si procede in modo analogo a quanto fatto con la dimostrazione della Proposizione 1.11, osservando che in tal caso la finitezza dell'estensione non è limitativa;

- $\Leftarrow$ Supponiamo ora E/F normale e separabile. Sia $\alpha \in E$ tale che $\sigma(\alpha) = \alpha$ per ogni $\sigma \in G := \mathrm{Gal}(E/F)$. Sia $p \in F[Y]$ il polinomio minimo di α su F . Allora p si decompone completamente sul campo E. Sia $L \subseteq E$ il campo di spezzamento del polinomio p. Allora per la Proposizione 1.11 segue che L/F è un'estensione di

Galois. Poniamo ora $H := Gal(L/F)$. Per il Lemma 1.13 segue che $\sigma(\alpha) = \alpha$ per ogni $\sigma \in H$. Poiché L/F è un'estensione di Galois possiamo concludere che $\alpha \in F$ e quindi E/F è un'estensione di Galois.

□

In analogia a quanto fatto con la Proposizione 1.11 è possibile mostrare che un'ulteriore condizione equivalente per definire un'estensione di Galois E/F è che E coincida con il campo di spezzamento di una famiglia di polinomi separabili su F.

1.3 Corrispondenza di Galois: caso finito

In questo capitolo introdurremo uno strumento di fondamentale importanza per la nostra trattazione: la corrispondenza di Galois; questa stabilisce una correlazione tra i sottogruppi del gruppo di Galois e i campi intermedi per una data estensione di campi di grado finito. Forniremo preliminarmente alcuni risultati, utili anche per la trattazione delle estensioni di Galois in dimensione infinita.

Lemma 1.15. *Sia E/F un'estensione di Galois e sia $F \subseteq M \subseteq E$ un sottocampo intermedio. Allora l'estensione E/M è di Galois.*

Dimostrazione. Mostriamo che E/M è normale e separabile: sia $\alpha \in E$ e sia $f \in M[Y]$ il polinomio minimo di α in M. consideriamo inoltre $g \in F[Y]$ il polinomio minimo di α su F. Osserviamo che, essendo E/F di Galois, g, ammette tutte le sue radici in E, inoltre $g \in F[Y] \subseteq M[Y]$, pertanto $f|g$. Poiché E/F è di Galois, g si spezza completamente su E, pertanto f ha tutte le sue radici in E, e in particolare sono distinte. □

Lemma 1.16. *Sia E/F un'estensione di Galois e sia $F \subseteq L \subseteq E$ un'estensione intermedia finita. Allora esiste un'estensione $L \subseteq M \subseteq E$ tale che M/F sia finita e di Galois.*

Dimostrazione. Per la Proposizione 1.14 l'estensione E/F è separabile, quindi lo è anche L/F, ma per ipotesi L/F è finita, pertanto, per il Teorema 1.8, esiste $\alpha \in L$ tale che $L = F(\alpha)$. Sia f il polinomio minimo di α su F; per quanto appena osservato f è separabile. Consideriamo M campo di spezzamento di f su F, allora, poiché E/F è normale, $L = F(\alpha) \subseteq M \subseteq E$. Abbiamo quindi mostrato che M/F è il campo di spezzamento di un polinomio separabile a coefficienti in F, perciò M/F è un'estensione di Galois. □

Lemma 1.17. *Sia E/F un'estensione di Galois e sia $F \subseteq L \subseteq E$ un'estensione intermedia. Allora L/F è di Galois se e solo se $\sigma(L) = L$ per ogni $\sigma \in Gal(E/F)$.*

Dimostrazione.

- $\Rightarrow$ Supponiamo L/F di Galois, e sia $\alpha \in L$; consideriamo $f \in F[Y]$ il polinomio minimo di α su F. Osserviamo che per ipotesi l'estensione L/F è normale, quindi tutte le radici di f sono in L. Sia σ un elemento generico di $\mathrm{Gal}(E/F)$, allora $\sigma(\alpha) \in root(f) \subseteq L$, da cui $\sigma(L) \subseteq L$. D'altra parte se consideriamo l'insieme $\{\alpha = \alpha_1, \alpha_2, ..., \alpha_n\}$ delle radici di f, si ha che σ agisce come una permutazione su tale insieme, e pertanto esiste α_i tale che $\sigma(\alpha_i) = \alpha$. Abbiamo in questo modo mostrato che $\sigma(L) = L$.
- $\Leftarrow$ Sia $G := \mathrm{Gal}(L/F)$ e proviamo che $F = L^G$.

$\subseteq$ Evidente dalla definizione di G;

$\supseteq$ Sia $\alpha \in L$; mostriamo che $\alpha \in L^G \Rightarrow \alpha \in F$, equivalentemente che $\alpha \notin F \Rightarrow \alpha \notin L^G$. Supponiamo quindi $\alpha \in L \setminus F$ e mostriamo che esiste $\sigma \in \mathrm{Gal}(L/F)$ tale che $\sigma(\alpha) \neq \alpha$. Sia f il polinomio minimo di α su F. Sia $\beta \in E$ una seconda radice di f. Definiamo allora una mappa

$$\begin{aligned} \gamma \colon F(\alpha) &\longrightarrow E \\ \alpha &\longmapsto \beta. \end{aligned}$$

Si verifica facilmente che γ è un F-morfismo, pertanto per il Lemma 1.13 è possibile estendere γ ad un automorfismo σ di E; in particolare $\sigma \in \mathrm{Gal}(E/F)$, dal momento che $\sigma_{|F} = \gamma_{|F} = id_{|F}$, ma allora $\sigma_{|_L} \in \mathrm{Gal}(L/F)$ e $\sigma(\alpha) = \beta \neq \alpha$.

□

Con queste premesse siamo ora in grado di enunciare il risultato principale riguardo le estensioni di Galois finite, ovvero il teorema di corrispondenza. Non daremo una prova esplicita di tale fatto. Si faccia riferimento a [1] per una dimostrazione completa;

Teorema 1.18. *(Corrispondenza di Galois per estensioni di campi finite). Sia E/F un'estensione di Galois finita e sia $G := Gal(E/F)$. Allora le mappe*

$$L \mapsto H := Gal(E/L) \qquad e \qquad H \mapsto L := E^H$$

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

Il Teorema appena enunciato si rivela molto utile in molteplici situazioni, dal momento che ci permette di estrapolare informazioni riguardo i campi intermedi di un'estensione di Galois a partire dai sottogruppi del gruppo di Galois associato, e viceversa. Vista l'utilità di questo teorema, vorremmo poterlo generalizzare al caso di estensioni di grado infinito. Avremo bisogno di alcuni strumenti preliminari, che tratteremo nei seguenti capitoli.

Capitolo 2

Gruppi topologici

Dopo aver richiamato brevemente alcune nozioni basilari di topologia generale riguardanti i prodotti topologici, introdurremo il concetto di gruppo topologico, prerequisito essenziale per poter comprendere la corrispondenza di Galois nel caso di estensioni infinite.

2.1 Richiami di topologia generale

Sia $\{X_i\}_{i\in I}$ una famiglia di spazi topologici, indichiamo con $X := \prod_{i\in I} X_i$ il loro prodotto cartesiano e con $\pi_i : X \to X_i$ le proiezioni canoniche. La topologia prodotto su X, che indicheremo con ξ, è definita come la meno fine fra tutte le topologie che rendono le proiezioni continue.

Osservazione 2.1. Sicuramente la topologia ξ descritta sopra esiste, in quanto è l'intersezione di tutte le topologie che rendono le proiezioni continue, e questa famiglia è non vuota in quanto almeno la topologia discreta gli appartiene.

Possiamo caratterizzare la topologia prodotto in modo più operativo, così come mostra la seguente proposizione.

Proposizione 2.2. *Sia $\{X_i\}_{i\in I}$ una famiglia di spazi topologici e ξ una topologia su $X := \prod_{i\in I} X_i$; sono equivalenti:*

1. *ξ coincide con la topologia prodotto su X;*
2. *Una prebase per ξ è data dagli insiemi del tipo $\pi_i^{-1}(U)$, dove $i \in I$ e U è un sottoinsieme aperto di X_i.*
3. *Una base per ξ è costituita dagli insiemi del tipo $\prod_{i\in I} A_i$, dove gli A_i sono aperti e coincidono con X_i tranne che per un numero finito di indici.*

Il risultato che andremo ora ad esporre è anche noto come "proprietà universale del prodotto topologico", e costituisce un'ulteriore caratterizzazione della topologia prodotto. Faremo largo uso di questo risultato per provare la maggior parte degli enunciati di questa sezione.

Proposizione 2.3 (Proprietà universale del prodotto topologico)**.** *Sia $\{X_i\}_{i\in I}$ una famiglia di spazi topologici, $X := \prod_{i\in I} X_i$ il loro prodotto cartesiano e dotiamo X della topologia prodotto ξ. Allora ξ è l'unica topologia su X che gode della seguente proprietà: per ogni spazio topologico Y e per ogni funzione $f : Y \to X$, f è continua se e soltanto se ogni $f_i := \pi_i \circ f$ è continua .*

2.2 Risultati elementari

Definizione 2.4. Un gruppo topologico è una terna $(G, \cdot, \tau)$, dove $(G, \cdot)$ è un gruppo e τ è una topologia su G tale che renda continue le mappe

$$\begin{aligned} \varphi\colon (G,\tau) &\longrightarrow (G,\tau) & \qquad \psi\colon (G\times G,\xi) &\longrightarrow (G,\tau) \\ g &\longmapsto g^{-1} & (g_1,g_2) &\longmapsto g_1 g_2 \end{aligned}$$

dove abbiamo indicato con ξ la topologia prodotto su $G \times G$.

Possiamo caratterizzare i gruppi topologici fornendo una definizione equivalente, come mostra la seguente proposizione:

Proposizione 2.5. *Sia G un gruppo e sia τ una topologia su G; sono equivalenti:*

- *(G, τ) è un gruppo topologico;*
- *la mappa*

$$\begin{aligned} \chi\colon (G\times G,\xi) &\longrightarrow (G,\tau) \\ (g_1,g_2) &\longmapsto g_1\cdot g_2^{-1} \end{aligned} \tag{2.1}$$

  è continua.

Dimostrazione. Ricordiamo che per la Proposizione 2.3 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. Supponiamo dapprima che (G, τ) sia un gruppo topologico. Osserviamo che le mappe

$$\begin{aligned} G\times G &\longrightarrow G & \qquad G\times G &\longrightarrow G \\ (g_1,g_2) &\longmapsto g_1 & (g_1,g_2) &\longmapsto g_2^{-1} \end{aligned}$$

sono continue, pertanto è continua anche la mappa

$$\begin{aligned} \theta\colon G\times G &\longrightarrow G\times G \longrightarrow G \\ (g_1,g_2) &\longmapsto (g_1,g_2^{-1}) \longmapsto g_1 g_2^{-1} \end{aligned}$$

dal momento che le restrizioni sulle componenti di $(g_1, g_2) \mapsto (g_1, g_2^{-1})$ sono continue e la mappa $(g_1, g_2^{-1}) \mapsto g_1 g_2^{-1}$ è continua per ipotesi. Supponiamo ora che valga la condizione 2.1; si ha immediatamente che la mappa $\varphi : G \to G$ definita da $g \mapsto 1 \cdot g^{-1}$ è continua. D'altra parte le mappe

$$\begin{aligned} (G\times G) &\longrightarrow G & \qquad G\times G &\longrightarrow G \\ g_1,g_2 &\longmapsto g_1 & (g_1,g_2) &\longmapsto g_2^{-1} \end{aligned}$$

sono continue, per definizione di topologia prodotto e dal momento che anche φ lo è. Sia ha pertanto che la composizione

$$\begin{aligned} \psi\colon G\times G &\longrightarrow G\times G \longrightarrow G \\ (g_1,g_2) &\longmapsto (g_1,g_2^{-1}) \longmapsto g_1(g_2^{-1})^{-1} = g_1 g_2 \end{aligned}$$

è continua, come richiesto. □

Proposizione 2.6. *Sia $\{G_i, \cdot_i, \tau_i\}$ una famiglia di gruppi topologici, allora lo spazio topologico $(\prod_i G_i, \cdot, \xi)$, dove $\cdot$ è l'operazione definita componente per componente, e ξ è la topologia prodotto, è un gruppo topologico.*

Dimostrazione. Mostriamo che la mappa

$$\begin{aligned} f : \prod G_i \times \prod G_i &\longrightarrow \prod G_i \\ ((x_i)_i, (y_i)_i) &\longmapsto (x_i y_i^{-1})_i \end{aligned}$$

è continua; sarà sufficiente mostrare la continuità di

$$\begin{aligned} f : \prod G_i \times \prod G_i &\longrightarrow G_j \\ ((x_i)_i, (y_i)_i) &\longmapsto (x_j y_j^{-1}). \end{aligned}$$

Definiamo la seguente composizione di mappe

$$\begin{aligned} \varphi_j : \prod G_i \times \prod G_i &\longrightarrow \prod G_j \longrightarrow G_j \\ ((x_i)_i, (y_i)_i) &\longmapsto (x_i)_i \longmapsto x_j \end{aligned}$$

e osserviamo che è continua per ogni j per definizione di topologia prodotto. Allo stesso modo poniamo

$$\begin{aligned} \psi_j : \prod G_i \times \prod G_i &\longrightarrow G_j \longrightarrow G_j \\ ((x_i)_i, (y_i)_i) &\longmapsto y_j \longmapsto y_j^{-1} \end{aligned}$$

che è continua per ogni j per quanto appena visto e poiché G_j è un gruppo topologico per ogni j. Allora

$$\begin{aligned} f : \prod G_i \times \prod G_i &\longrightarrow G_j \times G_j \\ ((x_i)_i, (y_i)_i) &\longmapsto \varphi_j((x_i)_i, (y_i)_i)), \psi_j((x_i)_i, (y_i)_i) \end{aligned}$$

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

$$\begin{aligned} \psi_j : \prod G_i \times \prod G_i &\longrightarrow G_j \times G_j \longrightarrow G_j \\ ((x_i)_i, (y_i)_i) &\longmapsto (x_j, y_j^{-1}) \longmapsto x_j y_j^{-1}. \end{aligned}$$

□

Osservazione 2.7. Se H è un sottogruppo di G ed H è munito della topologia indotta, allora H è un gruppo topologico.

Osservazione 2.8. Sia $(G, \cdot, \tau)$ un gruppo topologico, allora la mappa

$$\begin{aligned} \varphi : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

è un omeomorfismo

Proposizione 2.9. *Se g è un elemento di G allora le mappe*

$$\begin{aligned} \psi_g : G &\longrightarrow G & \qquad \psi'_g : G &\longrightarrow G \\ x &\longmapsto gx & x &\longmapsto xg \end{aligned}$$

sono omeomorfismi.

Dimostrazione. Mostriamo l'enunciato solo per ψ'_g, dal momento che il secondo caso è analogo. Poiché le mappe $x \mapsto g^{-1}$ e $x \mapsto x$ sono continue, si ha che

$$\begin{aligned} \psi'_g : G &\longrightarrow G \times G \longrightarrow G \\ x &\longmapsto (x, g^{-1}) \longmapsto xg \end{aligned}$$

è continua. Si verifica facilmente che ψ'_g è invertibile, con inversa data da $x \mapsto xg^{-1}$, che è continua per quanto appena mostrato. □

Capitolo 3

Gruppi profiniti

Discutiamo in questa sezione dapprima la costruzione dei limiti inversi, andando a considerare in particolare i limiti inversi di famiglie di gruppi finiti; mostreremo che tali oggetti sono a loro volta gruppi, e andremo a dotarli di una particolare topologia, così da poterli considerare come gruppi topologici. Le strutture così ottenute prendono il nome di gruppi profiniti, e si presentano naturalmente nella trattazione delle estensioni di Galois in dimensione infinita.

3.1 Sistemi e limiti inversi

Definizione 3.1. Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione 3.2. Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

In letteratura vengono utilizzati in modo interscambiabile i termini *"sistema inverso"* e *"famiglia proiettiva"* con riferimento in entrambi i casi alla definizione data qui sopra. Noi ci riferiremo a tali oggetti denotandoli sempre come *sistemi inversi*.

Esempio 3.3. Consideriamo $\mathbb{N}$ e la relazione $R \subseteq \mathbb{N} \times \mathbb{N}$ definita da $(m, n) \in R \Leftrightarrow m|n$; siano inoltre $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la mappa banale e φ_{nn} la mappa identica. Allora $\{\mathbb{Z}/n\mathbb{Z}, \varphi_{nm}\}$ costituisce un sistema inverso di gruppi.

Esempio 3.4. Consideriamo nuovamente $\mathbb{N}$ e la relazione $R \subseteq \mathbb{N} \times \mathbb{N}$ definita come sopra; per ogni $(m, n) \in R$ poniamo $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la mappa tale che $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$, e φ_{nn} la mappa identica. Allora $\{\mathbb{Z}/n\mathbb{Z}, \varphi_{nm}\}$ costituisce un sistema inverso di gruppi.

Esempio 3.5. Consideriamo un gruppo G, e sia Λ la famiglia dei suoi sottogruppi normali di indice finito. Per ogni $N \in \Lambda$ poniamo $G_N := G/N$. Sia ora $R \subseteq \Lambda \times \Lambda$ data da $(N_1, N_2) \in R \Leftrightarrow N_2 \subseteq N_1$. Osserviamo che se $N_1, N_2 \in \Lambda$, allora $N_1 \cap N_2 \in \Lambda$ e vale $(N_1, N_1 \cap N_2) \in R$ e $(N_2, N_1 \cap N_2) \in R$; poniamo infine $\varphi_{N_1 N_2} : G_{N_2} \to G_{N_1}$ la mappa $gN_2 \to gN_1$. Per quanto osservato $\{G_N, \varphi_{NM}\}$ è un sistema inverso di gruppi.

Osserviamo che negli Esempi 3.3 e 3.4 abbiamo utilizzato lo stesso insieme di indici, la stessa relazione R, e gli stessi gruppi, cambiando solamente le mappe φ_{nm}. È pertanto importante specificare sempre i morfismi di un sistema inverso.

Definizione 3.6. Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è un gruppo G, dotato degli omomorfismi $\varphi_a : G \to G_a$ tali che il diagramma

$$\begin{array}{ccc} G & \xrightarrow{\varphi_a} & G_a \\ {\scriptstyle \varphi_b}\downarrow & \nearrow_{\varphi_{ab}} & \\ G_b & & \end{array}$$

commuta per ogni $a \leq b$; richiederemo inoltre che per ogni $\{L, \psi_a\}$ con la precedente proprietà, $\exists!\ \chi : L \to G$ tale che

$$\begin{array}{ccccc} L & & \xrightarrow{\chi} & & G \\ & {\scriptstyle \psi_a}\searrow & & \swarrow{\scriptstyle \varphi_a} & \\ & & G_a & & \end{array}$$

commuta per ogni a.

Come prima, in letteratura vengono utilizzati in modo interscambiabile i termini *"limite inverso"* e *"limite proiettivo"*. Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}$ è denotato come $\varprojlim_{a \in \Lambda} G_a$, o più semplicemente con $\varprojlim G_a$, omettendo le mappe φ_a qualora siano già chiare dal contesto. Proveremo qui di seguito che per un sistema inverso di gruppi esiste sempre un limite inverso, e che tale limite è essenzialmente unico. Vedremo in particolare come nella dimostrazione di questo fatto venga costruito il limite inverso, permettendoci di darne una definizione più operativa.

Proposizione 3.7. *Sia $\{G_a, \varphi_{ab}\}$ un sistema inverso di gruppi, allora esiste sempre un limite inverso $\{G, \varphi_a\}$. Inoltre se $\{H, \psi_a\}$ è un altro limite inverso, allora la mappa $\chi : H \to G$ definita sopra è un isomorfismo di gruppi.*

Dimostrazione. Mostriamo dapprima che un limite inverso esiste sempre: definiamo

$$G := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b)\ \forall a \leq b \right\} \tag{3.1}$$

e poniamo $\varphi_a : G \to G_a$ la restrizione a G della mappa $\pi_a : \prod_{a \in \Lambda} G_a \to G_a$, che è chiaramente un omomorfismo. D'altronde $(\varphi_{ab} \circ \varphi_b)(g) = \varphi_{ab}(g_b) = g_a = \varphi_a(g)$ pertanto $\varphi_{ab} \circ \varphi_b = \varphi_a$ e la prima parte della Definizione 3.6 è verificata. Supponiamo ora che esista una collezione $\{H, \psi_a\}$ tale che ψ_a sia un omomorfismo e che per ogni $a \leq b$ si abbia $\varphi_{ab} \circ \psi_b = \psi_a$. Definiamo la mappa

$$\begin{aligned} \chi \colon H &\longrightarrow \textstyle\prod_{a \in \Lambda} G_a \\ h &\longmapsto (\psi_a(h))_{a \in \Lambda}. \end{aligned}$$

Osserviamo innanzitutto che $\pi_a \circ \chi = \psi_a$, infatti $\pi_a(\chi(h)) = \pi_a((\psi_a(h))_{a \in \Lambda}) = \psi_a(h)$. Si ha inoltre che χ è un omomorfismo, dal momento che ogni ψ_a lo è. Proviamo ora che l'immagine di χ è contenuta in G: se $a \leq b$, allora $\psi_a = \varphi_{ab} \circ \psi_b = \varphi_{ab} \circ (\pi_b \circ \chi)$; questo implica che $\chi(h) \in G$, in quanto soddisfa la specifica espressa dalla (3.1). Come immediata conseguenza abbiamo che $\varphi_a \circ \chi = \psi_a$, dal momento che $\varphi_a = (\pi_a)_{|_G}$. Infine, se $\chi' : H \to G$

è un altro omomorfismo che soddisfa $\varphi_a \circ \chi' = \psi_a$ per ogni $h \in H$ e $a \in \Lambda$, poiché vale anche $\varphi_a \circ \chi = \psi_a$ si ha $\varphi_a(\chi(h)) = \varphi_a(\chi'(h))$, ma allora la a-esima componente di $\chi(h)$ coincide con la a-esima componente di $\chi'(h)$, e questo vale per ogni $a \in \Lambda$, da cui segue $\chi(h) = \chi'(h)$, ovvero $\chi \equiv \chi'$.
Abbiamo in questo modo mostrato che un limite inverso esiste sempre; proviamone ora l'unicità. Siano $\{G, \varphi\}$ e $\{H, \psi_a\}$ due limiti inversi, allora sappiamo che esiste un'unica mappa $\chi_1 : H \to G$ tale che $\varphi_a \circ \chi_1 = \psi_a$ ed esiste un'unica mappa $\chi_2 : G \to H$ tale che $\varphi_a = \psi_a \circ \chi_2$, per ogni $a \in \Lambda$. Segue che $\psi_a = \psi_a \circ \chi_2 \circ \chi_1$ e $\varphi_a = \varphi_a \circ \chi_1 \circ \chi_2$, per ogni $a \in \Lambda$.

La proprietà universale descritta dalla Definizione 3.6 implica che esiste un'unica mappa $\sigma : G \to G$ tale che $\varphi_a = \varphi_a \circ \sigma$, ed esiste un'unica mappa $\tau : G \to G$ tale che $\psi_a = \psi_a \circ \tau$. Tuttavia, poiché 1_G soddisfa $\varphi_a = \varphi_a \circ 1_G$, e 1_H soddisfa $\psi_a = \psi_a \circ 1_H$, otteniamo $\chi_1 \circ \chi_2 = 1_G$ e $\chi_2 \circ \chi_1 = 1_H$, quindi $\chi_1 : H \to G$ è un isomorfismo. □

Osservazione 3.8. Per quanto appena visto possiamo caratterizzare il limite di un sistema proiettivo come

$$\varprojlim_{a \in \Lambda} G_a = \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \ \forall a \leq b \right\}.$$

Osserviamo inoltre che sussistono dei naturali omomorfismi $\varprojlim_a G_a \to G_{a'}$ per ogni $a' \in \Lambda$. Usando queste mappe, il limite inverso soddisfa una proprietà universale, che enunciamo per completezza, ma di cui non forniremo una dimostrazione.

Proposizione 3.9. *Sia $\{G_a\}$ un sistema inverso di gruppi, e sia H un gruppo generico. La composizione con le mappe $\varprojlim_a G_a \to G_{a'}$ induce un iniezione*

$$Hom(H, \varprojlim_a G_a) \hookrightarrow \prod_{a \in \Lambda} Hom(H, G_a),$$

dove l'immagine è costituita esattamente dalle uple $\gamma_a : H \to G_a$ tali che per ogni $a \leq b$ si abbia $\varphi_{ab} \circ \gamma_b = \gamma_a$.

Esempio 3.10. Sia Λ un insieme, e consideriamo la relazione banale su $\Lambda \times \Lambda$, ovvero $R = \emptyset$, allora il limite inverso del corrispondente sistema inverso non è altro che il prodotto.

Esempio 3.11. Consideriamo $\{\mathbb{Z}/p^n\mathbb{Z}, \varphi_{nm}\}$, ove $\varphi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, con $n \leq m$, è la proiezione naturale. Tale struttura definisce un sistema inverso. Denotiamo con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ \{a_i\} \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_o + pa_1 + p^2a_2 & & \cdots \end{array}$$

che identifichiamo come la serie $\sum_{n \in \mathbb{N}} a_n p^n$. Gli elementi dell'anello $\mathbb{Z}_p$ sono detti interi p-adici.

Esempio 3.12. Nel caso dell'Esempio 3.4 il limite inverso è $\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$ e si può mostrare che coincide con $\prod_p \mathbb{Z}_p$, dove $\mathbb{Z}_p := \left\{\{a_i\} \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti}\right\}$, ovvero con il prodotto diretto degli interi p-adici su tutti i primi p. Riprenderemo più avanti questo concetto.

Osservazione 3.13. Si osserva immediatamente che il limite di un sistema inverso di gruppi è effettivamente un sottogruppo del prodotto.

3.2 Sistemi e limiti diretti

Il procedimento con cui abbiamo costruito i sistemi e i limiti inversi può essere ripercorso in maniera duale per costruire i sistemi e i limiti diretti. Non daremo particolare risalto a tali strutture algebriche dal momento che non sono essenziali per la trattazione, e le descriveremo unicamente per completezza espositiva

Definizione 3.14. Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema diretto di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a\leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_a \to G_b$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{bc}} & G_c \\ {\scriptstyle\varphi_{ab}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_a & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Definizione 3.15. Un limite diretto del sistema diretto $\{G_a, \varphi_{ab}\}_{a\leq b}$ è un gruppo G, dotato degli omomorfismi $\varphi_a : G_a \to G$ tali che il diagramma

$$\begin{array}{ccc} G_a & \xrightarrow{\varphi_a} & G \\ {\scriptstyle\varphi_{ab}}\downarrow & \nearrow_{\varphi_b} & \\ G_b & & \end{array}$$

commuta per ogni $a \leq b$; richiederemo inoltre che per ogni $\{L, \psi_a\}$ con la precedente proprietà, $\exists!\ \chi : L \to G$ tale che

$$\begin{array}{ccccc} L & & \xrightarrow{\chi} & & G \\ & {\scriptstyle\psi_a}\nwarrow & & \nwarrow{\scriptstyle\varphi_a} & \\ & & G_a & & \end{array}$$

commuta per ogni a.

Il limite diretto è in genere denotato come $\varinjlim G_a$, lasciando sottinteso il sistema diretto $\{G_a, \varphi_{ab}\}_{a\leq b}$. Analogamente a quanto mostrato per i limiti inversi, si verifica che se esiste un limite diretto, allora esso è unico, nel senso che tutti i limiti diretti di un sistema diretto sono isomorfi tra loro.

Esempio 3.16. Una collezione di sottoinsiemi M_i di un insieme M può essere parzialmente ordinata dall'inclusione. Se per ogni coppia di sottoinsiemi A e B, con $A \subseteq B$, definiamo il morfismo da A a B come l'inclusione canonica, allora il limite diretto risultante da questo sistema non è altro che l'unione degli M_i.

Esempio 3.17. Sia p un primo. Si consideri il sistema diretto composto dai gruppi $\mathbb{Z}/p^n\mathbb{Z}$ e dagli omomorfismi $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, con $n \leq m$, che sono indotti dalla moltiplicazione per p^{m-n}. Il limite diretto di questo sistema è isomorfo al gruppo di tutte le radici dell'unità di ordine una qualche potenza di p, ed è chiamato gruppo di Prüfer $\mathbb{Z}(p^\infty)$.

3.3 Gruppi profiniti

Definizione 3.18. Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti, e dotiamo ogni G_a della topologia discreta. Allora dotiamo $\prod G_a$, della topologia prodotto ξ, e il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ. In questa sezione quando ci riferiremo a un gruppo profinito lo considereremo sempre dotato della topologia ottenuta con questa costruzione.

Osservazione 3.19. Come abbiamo anticipato nel capitolo precedente, si poteva definire questa topologia in modo equivalente come quella topologia che ha come prebase gli aperti della forma $\pi_a^{-1}(U)$ al variare di $a \in \Lambda$ e di U tra gli aperti di G_a. La necessità di introdurre la nozione di prebase viene proprio dall'esigenza di definire una buona topologia in un prodotto infinito di spazi topologici, infatti non si può procedere come nel caso finito, scegliendo come base di $\prod G_a$ gli aperti nella forma $\prod U_a$, con U_a sottoinsieme aperto di G_a, in quanto ci sarebbero troppi aperti. Per rendere le proiezioni continue è sufficiente considerare aperti solo prodotti della forma $\prod U_a$ con solo un numero finito di U_a diversi da G_a, in quanto questo basta a garantire che le intersezioni finite di aperti siano aperte. Chiaramente questa definizione coincide con quella usuale di prodotto nel caso di prodotti finiti.

Proposizione 3.20. *Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.*

Dimostrazione. La topologia che abbiamo definito su G , ammette per costruzione una pre-base costituita dagli insiemi della forma $\pi_a^{-1}(\{g_a\})$, al variare di $a \in G_a$, di conseguenza una pre-base per G può essere espressa dalla famiglia di aperti $\{G \cap \pi_a^{-1}(\{g_a\})\}$. Fatta questa premessa risulta chiaro che per provare l'asserto è sufficiente mostrare che la controimmagine di un qualsiasi aperto del tipo $\pi_a^{-1}(\{g_a\})$ secondo le mappe prodotto $p : G \times G \to G$ e inversa $i : G \to G$ sia ancora un aperto. Sia $\pi_a^{-1}(\{g_a\})$ un tale aperto; proviamo che

$$p^{-1}(\pi_a^{-1}(\{g_a\})) = \bigcup_{h \in G_a} \pi_a^{-1}(\{g_a h\}) \times \pi_a^{-1}(\{h^{-1}\}),$$

il quale è chiaramente un aperto nella topologia prodotto di $G \times G$.
Sia dapprima $(g_1, g_2) \in p^{-1}(\pi_a^{-1}(\{g_a\}))$, allora $g_1 g_2 \in \pi_a^{-1}(\{g_a\})$ e

$$\pi_a(g_1 g_2) = \pi_a(g_1)\pi_a(g_2) = (g_1)_a (g_2)_a = g_a,$$

segue che $(g_1)_a = g_a (g_2)_a^{-1}$, ovvero, ponendo $h := (g_2)_a^{-1}$, $g_1 \in \pi_a^{-1}(\{g_a h\})$, e $(g_2)_a = h^{-1}$, pertanto $g_2 \in \pi_a^{-1}(\{h\})$. Viceversa sia $(a, b) \in \bigcup_{h \in G_a} \pi_a^{-1}(\{g_a h\}) \times \pi_a^{-1}(\{h^{-1}\})$, allora $\pi_a(ab) = \pi_a(a)\pi_a(b) = (g_a h)(h^{-1}) = g_a$, ovvero $(a, b) \in \pi_a^{-1}(\{g_a\})$. Similmente si verifica che $i^{-1}(\pi_a^{-1}(\{g_a\})) = \pi_a^{-1}(\{g_a^{-1}\})$, che è chiaramente aperto nella topologia di G, da cui la tesi. □

Lemma 3.21. *Sia (G_a, φ_{ab}) un sistema inverso di gruppi topologici finiti equipaggiati con la topologia discreta. Allora il limite inverso $G := \varprojlim G_a$ è chiuso in $P := \prod G_a$.*

Dimostrazione. Mostriamo che $P \setminus G$ è aperto: sia $g = (g_a)_a \in P \setminus G$ e siano pertanto i, j tali che $\varphi_{ij}(g_j) \neq g_i$. Poniamo $A := \{(h_a) \in P : h_i = g_i \text{ e } h_j = g_j\}$. Chiaramente $A \cap G = \emptyset$. Resta da provare che U è aperto. Poste $p_k : P \to G_k$ le proiezioni canoniche, si ha che $U = p_i^{-1}(\{g_i\}) \cap p_j^{-1}(\{g_j\})$ ed è quindi aperto perché le proiezioni sono continue e i G_a discreti. □

Corollario 3.22. *Un gruppo profinito è compatto*

Dimostrazione. Dato che gli spazi finiti sono compatti, per il teorema di Tichonov lo è anche il loro prodotto. Allora G è, per il lemma 3.21, un sottoinsieme chiuso di uno spazio compatto, quindi è a sua volta compatto. □

Corollario 3.23. *I sottogruppi aperti di G sono tutti e soli i suoi sottogruppi chiusi di indice finito*

Dimostrazione. Sia A un sottogruppo aperto di G, allora il suo complementare è unione delle sue classi laterali gA, ovvero $G \setminus A = \bigcup_{g \notin A} gA$. Per la Proposizione 2.9 si ha che la moltiplicazione per elementi di G è un omeomorfismo, pertanto gli insiemi gA sono aperti, da cui segue che A è chiuso. Poiché $G = \bigcup_g gA$, e G è compatto, l'indice di A in G è finito. Viceversa, sia F un sottogruppo di G, chiuso e di indice finito. Allora F è il complementare dell'unione finita delle sue classi laterali, che sono chiuse, quindi è aperto. □

Proposizione 3.24. *I sottogruppi chiusi di G sono intersezione di sottogruppi aperti. I sottogruppi chiusi e normali di G sono intersezione di sottogruppi aperti normali.*

Dimostrazione. Sia H un sottogruppo chiuso di G. Indichiamo con $(G_i)_{i \in I}$ l'insieme di gruppi tale che $G = \varprojlim G_i$; siano inoltre $\pi_i : G \to G_i$ le proiezioni naturali e $\{U_j\}_{j \in J}$ la famiglia di tutti i sottogruppi aperti e normali di G. Dal momento che $ker(\pi_i)$ è un sottogruppo normale di G, per ogni $i \in I$, allora $\{ker(\pi_i)\}_{i \in I} \subseteq \{U_j\}_{j \in J}$; ne segue che $\bigcap U_j \subseteq \bigcap Ker(\pi_i) = \{1\}$, e quindi $\bigcap U_j = \{1\}$.
Osserviamo anche che $HU_j := \{hu : h \in H, u \in U_j\} = \bigcup_{h \in H} hU_j$, pertanto, per quanto visto con i gruppi topologici, tale insieme è sicuramente aperto in G (è anche normale, se H lo è).
Proviamo ora che $H = \bigcap_j HU_j$:

- $\subseteq$ $H = H \cdot 1 = H \cdot \bigcap U_j \subseteq \bigcap HU_j$
- $\supseteq$ Sia $g \in \bigcap_j HU_j$; se per assurdo $g \notin H$, allora anche $g^{-1} \notin H$, da cui $1 \notin Hg$, quindi $Hg \cap \{1\} = Hg \cap \bigcap U_j = \emptyset$. Segue quindi che $(Hg)^c \cup \bigcup_{j \in J} U_j^c = G$. Per l'ipotesi di compattezza di G esiste un sottoinsieme finito $J_0 \subseteq J$ tale che $(Hg)^c \cup \bigcup_{j \in J_0} U_j^c = G$, da cui $Hg \cap \bigcap_{j \in J_0} U_j = \emptyset$. Ma ora $N := \bigcap_{j \in J_0} U_j$ è un sottogruppo aperto (e normale, se H lo è) di G, essendo intersezione di un numero finito di aperti. In particolare $N \in \{U_j\}$ e pertanto, per ipotesi, $g \in HN$. Esistono quindi $h \in H$ e $n \in N$ tali che $g = hn$. Ma allora $Hg \ni h^{-1}g = n \in N$, quindi $Hg \cap N \neq \emptyset$, il che è assurdo.

□

Proposizione 3.25. *Sia $G := \varprojlim G_i$ un gruppo profinito e siano $\pi_i : G \to G_i$ le proiezioni naturali. Allora $ker(\pi_i)$ è un sistema fondamentale di intorni di $1 \in G$.*

Dimostrazione. Indichiamo con 1_i l'elemento neutro di G_i e con $p_j : \prod G_i \to G_j$ le proiezioni canoniche. Per la definizione di topologia prodotto e discretezza dei G_i si ha che gli insiemi della forma $\left(\bigcap_{i \in I_0} ker(p_i)\right)$, al variare un qualche sottoinsieme finito I_0 di I, formano un sistema fondamentale di intorni di 1 in $\prod G_i$. Segue che un sistema fondamentale di intorni di 1 in G è dato dagli insiemi della forma $G \cap \bigcap_{i \in I_0} ker(p_i) = \bigcap_{i \in I_0} G \cap ker(p_i) = \bigcap_{i \in I_0} ker(\pi_i)$. Mostriamo che più in particolare $\{ker(\pi_j)\}_{j \in I}$ è un sistema fondamentale di intorni per 1: sia fissato un insieme del tipo $\bigcap_{i \in I_0} ker(\pi_i)$, allora, dato che I è diretto, esiste $j \in I$ tale che $i \leq j$ per gni $i \in I_0$. Si ha quindi che $ker(\pi_j) \subseteq ker(\pi_i)$ per ogni $i \in I_0$, da cui segue immediatamente $ker(\pi_j) \subseteq \bigcap_{i \in I_0} ker(\pi_i)$, da cui la tesi. □

Proposizione 3.26. *Sia $G := \varprojlim_{i\in I} G_i$ un gruppo profinito, dove i G_i formano un sistema inverso di gruppi finiti. Sia $H \subseteq G$ un sottogruppo. Allora H è aperto se e solo se esiste $i \in I$ e un sottogruppo $H_i \subseteq G_i$ tale che H coincida con la preimmagine di H_i sotto la mappa di proiezione $G \to G_i$*

Dimostrazione. Dal momento che la mappa $G \to G_i$ è continua e ogni G_i è dotato della topologia discreta, la preimmagine in G di qualsiasi sottoinsieme di G_i è sicuramente aperta. Viceversa, supponiamo H aperto in G, allora H è chiuso, e quindi compatto. Di conseguenza è possibile ricoprire H con un numero finito di aperti della forma $H \cap \prod_{i\in I} U_i$, dove $U_i = G_i$ a parte che per un numero finito di termini. Per come abbiamo definito il limite inverso ognuno di questi insiemi può essere scritto con un solo $U_j \neq G_i$. Poiché H è unione finita di tali insiemi, può essere scritto nello stesso modo, con un singolo $U_i \neq G_i$. Ma $G \to G_i$ è un omomorfismo di gruppi, quindi l'immagine di H coincide con un sottogruppo $H_i \subseteq G_i$. Abbiamo in questo modo mostrato che H è la preimmagine di un sottogruppo $H_i \subseteq G_i$, come richiesto. □

3.4 Il gruppo di Galois come gruppo profinito

Di seguito proviamo che data un'estensione di Galois infinita E/F, i gruppi di Galois delle sottoestensioni di Galois finite, assieme alle suriezioni naturali $\varphi_{LM} : \mathrm{Gal}(M/F) \to \mathrm{Gal}(L/F)$ formano un sistema inverso.

Proposizione 3.27. *Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.*

Dimostrazione. Siano $f, g \in F[Y]$ due polinomi separabili tali che L e M siano i campi di spezzamento di f e g, rispettivamente. Allora il polinomio fg è separabile, e ha tutte le rue radici in LM. Mostriamo che LM è il campo di spezzamento di fg: supponiamo $F \subseteq N \subseteq E$ un'estensione tale che contenga tutte le radici di fg, allora N contiene tutte le radici di f, quindi contiene L, e allora stesso modo contiene M, da cui $LM \subset N$. Abbiamo in questo modo mostrato che LM/F è anche finita, e quindi di Galois. □

Con questa proposizione abbiamo provato che l'insieme $(G_a)_{a\in\Lambda}$ delle estensioni finite e di Galois su F, non solo è parzialmente ordinato dalle inclusioni, ma è anche diretto. Possiamo pertanto affermare che data un'estensione di Galois E/F i gruppi di Galois delle sottoestensioni di Galois finite, assieme con le suriezioni naturali $\varphi_{LM} : \mathrm{Gal}(M/F) \to \mathrm{Gal}(L/F)$ formano un sistema inverso. Mostriamo ora che ogni gruppo di Galois è un gruppo profinito.

Proposizione 3.28. *Sia E/F un'estensione di Galois. Allora*

$$Gal(E/F) \cong \varprojlim_{M\in\Lambda} Gal(M/F),$$

dove abbiamo indicizzato con Λ l'insieme di tutte le sottoestensioni di E finite e di Galois su F.

Dimostrazione. Definiamo una mappa

$$\begin{aligned} \varphi\colon \mathrm{Gal}(E/F) &\longrightarrow \textstyle\prod_{L\in\Lambda} \mathrm{Gal}(L/F) \\ \sigma &\longmapsto (\sigma_{|_L})_{L\in\Lambda}. \end{aligned}$$

Per il Lemma 1.17 si ha che φ è ben definita, ed è un morfismo di gruppi, dal momento che $\varphi(\sigma \circ \tau) = ((\sigma \circ \tau)_{|L})_{L\in\Lambda} = (\sigma_{|_L} \circ \tau_{|_L})_{L\in\Lambda} = (\sigma_{|_L})_{L\in\Lambda} \circ (\tau_{|_L})_{L\in\Lambda} = \varphi(\sigma) \circ \varphi(\tau)$. Mostriamo ora che $\mathrm{Im}(\varphi) = \varprojlim \mathrm{Gal}(M/F)$.

- $\subseteq$ Sia $\varphi(\sigma) = (\sigma_{|_L})_{L\in\Lambda} \in \mathrm{Im}(f)$, e siano $L \subseteq M$ due estensioni finite e di Galois su F; allora $\varphi_{LM}(\sigma_{|_M}) = (\sigma_{|_M})_{|_L} = \sigma_{|_L}$.
- $\supseteq$ Sia $(\sigma_L)_{L\in\Lambda}$, definiamo allora un automorfismo $\sigma \in \mathrm{Gal}(E/F)$ come segue: se $\alpha \in E$, allora per il Lemma 1.16 esiste $M \in \Lambda$ tale che $F(\alpha) \subset M$, in particolare avremo che $\alpha \in M$; poniamo $\sigma(\alpha) := \sigma_M(\alpha)$. Per come abbiamo costruito $\varprojlim \mathrm{Gal}(M/F)$ si ha che tale morfismo è ben definito, e vale $\varphi(\sigma) = (\sigma_L)_{L\in\Lambda}$, dal momento che $\varphi(\sigma)_{|_L} = \sigma_L$ per ogni $L \in \Lambda$.

Resta da vedere che φ è iniettiva, equivalentemente che $ker(\varphi) = \{1_E\}$.

- $\supseteq$ Naturalmente $1_E \in ker(\varphi)$;
- $\subseteq$ Sia $1_E \neq \sigma \in \mathrm{Gal}(E/F)$, allora esiste $\alpha \in E$ tale che $\sigma(\alpha) \neq \alpha$. Per il Lemma 1.16 possiamo considerare $M \in \Lambda$ contenente $F(\alpha)$. Osserviamo che $\sigma_{|_M} \neq 1_M$, quindi $\varphi(\sigma)$ ha almeno una componente non banale e non è l'identità, da cui segue $\sigma \notin ker(\varphi)$.

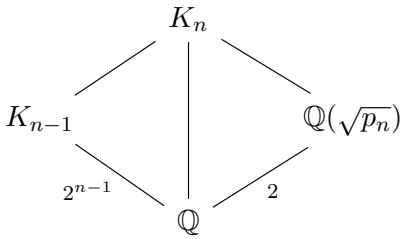
Abbiamo in questo modo mostrato che $\varphi : \mathrm{Gal}(E/F) \to \varprojlim \mathrm{Gal}(L/F)$ è iniettiva, da cui segue $\mathrm{Gal}(E/F) \cong \varprojlim \mathrm{Gal}(L/F)$. □

Dalla dimostrazione appena fatta risulta chiaro che per ottenere tale risultato non è strettamente necessario indicizzare su Λ tutte le estensioni finite e di Galois su F, ma è sufficiente un sottoinsieme di Λ costituito da estensioni finite e di Galois su F tali che la loro unione coincida con E. Vediamo alcuni esempi in cui questa caratterizzazione dei gruppi di Galois è utile.

Esempio 3.29. Se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora:

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$$

Si può infatti provare tale fatto per induzione su n; il caso $n = 1$ è evidente. Se $n > 1$, consideriamo il diagramma.



Osserviamo che sarà sufficiente provare che $\mathbb{Q}(\sqrt{p_n}) \nsubseteq K_{n-1}$. Le sottoestensioni di K_{n-1} di grado 2 sono tante quanti i sottogruppi di $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ di indice 2, cioè $2^{n-1} - 1$. Ma le sottoestensioni del tipo $\mathbb{Q}(\sqrt{p_1^{\epsilon_1}...p_{n-1}^{\epsilon_{n-1}}})$, con $\epsilon_i \in \{0, 1\}$ sono esattamente 2^{n-1} ($2^{n-1} - 1$ se non si conta $\mathbb{Q}$) e sono tutte distinte, in quanto due estensioni quadratiche $\mathbb{Q}(\sqrt{n})$ e $\mathbb{Q}(\sqrt{m})$ di $\mathbb{Q}$ sono la stessa se e solo se nm è un quadrato. Segue perciò che $\mathbb{Q}(\sqrt{p_n})$ non è una sottoestensione di K_{n-1}, cioè la tesi.

Esempio 3.30. Sia $K = \mathbb{Q}(\{\sqrt{p} \,|\, p \text{ primo}\})$, allora $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$, ma visto che i K_n sono una sottofamiglia filtrante delle F_i , cioè $\forall\, i\, \exists\, n$ tale che $F_i \subseteq K_n$, allora $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$. Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(K_n/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/2\mathbb{Z})^n \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z},$$

in quanto si identifica una successione in $(\mathbb{Z}/2\mathbb{Z})^n$ con il suo elemento limite in $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

Per il prossimo esempio abbiamo bisogno di introdurre un risultato preliminare dovuto a Kronecker e Weber, la cui dimostrazione va oltre lo scopo del nostro discorso.

Teorema 3.31. *Sia $K/\mathbb{Q}$ un'estensione finita di campi. Allora $K/\mathbb{Q}$ è abeliana se e solo se K è contenuto in un'estensione ciclotomica di $\mathbb{Q}$.*

Esempio 3.32. Consideriamo l'estensione $\mathbb{Q}_{ab}/\mathbb{Q}$, dove abbiamo indicato con $\mathbb{Q}_{ab}$ la più grande estensione abeliana di $\mathbb{Q}$. Per il teorema 3.31 otteniamo che $\mathbb{Q}_{ab} = \mathbb{Q}(\{\zeta_n | n \in \mathbb{N}\})$, inoltre questo è il campo di spezzamento di una famiglia di polinomi separabili, e pertanto $\mathbb{Q}_{ab}/\mathbb{Q}$ è di Galois. Chiaramente un elemento $\sigma \in G := \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q})$ è univocamente determinato dal suo comportamento sull'insieme $\{\zeta_n : n \in \mathbb{N}\}$. È inoltre un fatto noto che σ mappi ζ_n in un'altra radice del suo polinomio minimo, in particolare $\sigma(\zeta_n) = \zeta_n^k$, con $(k, n) = 1$, così come è noto che per estensioni ciclotomiche si abbia $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Consideriamo la famiglia $\{G_n := (\mathbb{Z}/n\mathbb{Z})^\times\}$, parzialmente ordinata dalla relazione $m \leq n \Leftrightarrow m|n$. Si prova facilmente che se $m|n$, allora esiste $d \in \mathbb{N}$ tale che $\zeta_m = \zeta_n^d$, e pertanto $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$; possiamo quindi definire una mappa

$$\begin{aligned} \phi_{mn} \colon \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \sigma &\longmapsto \sigma_{|_{\mathbb{Q}(\zeta_n)}}. \end{aligned}$$

Poiché sotto queste ipotesi se $\sigma(\zeta_n) = \zeta_n^k$, allora $\sigma(\zeta_m) = \sigma(\zeta_n^d) = \sigma(\zeta_n)^d = \zeta_n^{kd} = \zeta_m^k$; guardando i vari σ_n come elementi di $\mathbb{Z}/n\mathbb{Z}$ possiamo affermare $\sigma_n \equiv \sigma_m \bmod(m)$. Questo implica che possiamo vedere ϕ_{mn} come la mappa $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$. Abbiamo in questo modo provato che $\mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^\times$, che è isomorfo al gruppo $\hat{Z}^\times$ delle unità di $\hat{Z}$.

Esempio 3.33. Consideriamo il campo $F := \mathbb{C}(x)$, definiamo $S := \{\sqrt[n]{x} : n \in \mathbb{N}\}$ e poniamo $K := F(S)$. Chiaramente K/F è di Galois dal momento che coincide con il campo di spezzamento della famiglia di polinomi $\{Y^n - x \in F[Y] : n \in \mathbb{N}\}$, ed è quindi normale, ma K/F è un'estensione di campi di caratteristica 0, ed è pertanto anche separabile. È possibile mostrare (si faccia riferimento a [5] per ulteriori dettagli) che per ogni estensione finita $F \subseteq E \subseteq K$, dove $E = F(\sqrt[n]{x})$, vale $\mathrm{Gal}(E/F) \cong \mathbb{Z}/n\mathbb{Z}$. Osserviamo inoltre che se $m|n$ (supponiamo $n = md$), allora se $\sigma \in \mathrm{Gal}(K/F)$ è tale che $\sigma(\sqrt[n]{x}) = \zeta_n^k \sqrt[n]{x}$, allora $\sigma(\sqrt[m]{x}) = \sigma(\sqrt[n]{x}^d) = \zeta_n^{kd} \sqrt[n]{d} = \zeta_m^k \sqrt[m]{x}$. In questo modo possiamo vedere che $\mathrm{Gal}(K/F) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}$, dove l'insieme $\mathbb{N}$ è parzialmente ordinato dalla relazione $m \leq n \Leftrightarrow m|n$, e per ogni $m \leq n$ abbiamo i morfismi $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dati da $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$. Abbiamo ottenuto ancora una volta che $\mathrm{Gal}(K/F) \cong \hat{\mathbb{Z}}$.

3.5 Topologia di Krull

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrispondenza come nel Teorema 1.18, infatti in generale esistono sottogruppi di $\mathrm{Gal}(E/F)$ che non corrispondono a nessuna estensione di F, come mostra l'esempio seguente.

Esempio 3.34. Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$. K è il campo di spezzamento della famiglia di polinomi separabili $\{x^2 - p \mid p \text{ primo}\}$, pertanto $K/\mathbb{Q}$ è un'estensione di Galois infinita. Dal momento che ogni $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ mappa $\sqrt{p}$ in una radice del suo polinomio minimo, ovvero $x^2 - p$, otteniamo $\sigma(p) \in \{\sqrt{p}, -\sqrt{p}\}$; fatta questa considerazione, ricordando quanto visto con gli ultimi esempi della sezione precedente, si ha che $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$ e pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$, che deve avere cardinalità maggiore di quella di V, è più che numerabile. Un'immediata conseguenza di tale fatto è che $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile, infatti se $\phi_1, \phi_2 \in V^*$, con $\phi_1 \neq \phi_2$, allora esiste $v \in V$ tale che $\phi_1(v) \neq \phi_2(v)$; senza perdita di generalità supponiamo $\phi_1(v) = 0$ e $\phi_2(v) = 1$. Allora $\ker(\phi_1) \ni v \notin \ker(\phi_2)$, e pertanto $\ker(\phi_1) \neq \ker(\phi_2)$. Osserviamo per ogni ϕ vale $V/\ker(\phi) \cong \mathbb{F}_2$. Abbiamo pertanto che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.
Tuttavia, seguendo la logica del Teorema 1.18, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con l'insieme delle estensioni quadratiche di $\mathbb{Q}$, ma tale insieme è dato da $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile, da cui segue che non può sussistere una corrispondenza biunivoca fra sottocampi di $\mathbb{Q}(S)$ e sottogruppi di $\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$ cosi come descritta dal teorema fondamentale.

Risolveremo questo problema considerando solamente i sottogruppi chiusi di $\mathrm{Gal}(E/F)$ in un'opportuna topologia, che andremo ora a descrivere.

Definizione 3.35. (topologia di Krull) Dotiamo ogni $\mathrm{Gal}(M/F)$ della topologia discreta e consideriamo $(\prod \mathrm{Gal}(M/F), \xi)$, dove abbiamo indicato con ξ la topologia prodotto. Chiameremo topologia di Krull la topologia indotta da $(\prod \mathrm{Gal}(M/F), \xi)$ sul sottogruppo $\varprojlim \mathrm{Gal}(M/F)$.

Osserviamo che questa topologia coincide con quella introdotta al paragrafo precedente, pertanto per una generica estensione di Galois valgono tutti gli i risultati enunciati nella sezione precedente per i gruppi profiniti, in particolare dalla Proposizione 3.20 segue immediatamente il seguente risultato.

Corollario 3.36. *Sia E/F un'estensione di Galois, e τ la topologia di Krull su $Gal(E/F)$. Allora $(Gal(E/F), \tau)$ è un gruppo topologico.*

Capitolo 4

Corrispondenza di Galois per estensioni di grado infinito

Abbiamo ora tutti gli strumenti per poter descrivere la corrispondenza di Galois nel caso di estensioni infinite di campi.

4.1 Corrispondenza di Galois: caso infinito

Teorema 4.1. *Sia E/F un'estensione di Galois infinita e sia $G := Gal(E/F)$. Allora le mappe*

$$L \mapsto H := Gal(E/L) \qquad e \qquad H \mapsto L := E^H$$

inducono una biiezione fra i sottocampi intermedi di E/F e i sottogruppi chiusi di G che rovescia le inclusioni. L'estensione L/F è di Galois se e solo se H è normale in G e in tal caso si ha $Gal(L/F) \cong G/H$. L'estensione L/F è finita se e solo se H è un sottogruppo aperto di G.

Dimostrazione. Mostriamo innanzitutto che se L è un campo intermedio finito su F, allora $\mathrm{Gal}(E/L)$ è sia aperto che chiuso in G. Per il Lemma 1.16 possiamo considerare $L \subseteq M \subseteq E$ finita e i Galois su F. Allora $\mathrm{Gal}(M/F)$ è uno dei gruppi del sistema inverso che ha come limite G, pertanto sussite una suriezione naturale $\pi_M : G \to \mathrm{Gal}(M/F)$ data dalla proiezione sulle componenti. Per il Teorema fondamentale nel caso finito si ha che $\mathrm{Gal}(M/L)$ è un sottogruppo di $\mathrm{Gal}(M/F)$. Sia $U_L := \pi_M^{-1}\mathrm{Gal}(M/L)$, allora

- U_L è aperto dal momento che π_M è continua e $\mathrm{Gal}(M/F)$ è discreto;
- $U_L = \mathrm{Gal}(E/L)$, infatti ogni elemento di U_L coincide con l'identità su L, perché controimmagine di un elemento di $\mathrm{Gal}(M/L)$. Viceversa sia $\sigma \in \mathrm{Gal}(E/L)$, allora $\pi_M(\sigma) \in \mathrm{Gal}(M/L)$, da cui segue $\pi_M(\mathrm{Gal}(E/L)) \subseteq \mathrm{Gal}(M/L)$, e quindi $\mathrm{Gal}(E/L) \subseteq \pi_M^{-1}(\pi_M(\mathrm{Gal}(E/L))) \subseteq \pi_M^{-1}(\mathrm{Gal}(M/L)) = U_L$. Abbiamo in questo modo mostrato che $\mathrm{Gal}(E/L)$ è aperto in G, da cui segue, per il Lemma 3.23, che $\mathrm{Gal}(E/L)$ è anche chiuso in G.

Sia ora $F \subseteq L \subseteq E$ un'estensione arbitraria di F. Chiaramente vale $L = \bigcup_{\alpha \in L} F(\alpha)$ e ogni estensione $F(\alpha)/F$ è finita. Segue che

$$\mathrm{Gal}(E/L) = \mathrm{Gal}(E/\bigcup_{\alpha \in L} F(\alpha)) = \bigcap_{\alpha \in L} \mathrm{Gal}(E/F(\alpha)).$$

Ma ognuno dei $\mathrm{Gal}(E/F(\alpha))$ è chiuso, per quanto mostrato sopra, pertanto $\mathrm{Gal}(E/L)$ è chiuso, essendo intersezione arbitraria di chiusi. Dato che E/L è di Galois per il Lemma 1.15, si ha $E^{Gal(E/L)} = L$.
Viceversa, sia H un sottogruppo chiuso di G e sia $L := E^H$. Chiaramente $F \subseteq L \subseteq E$ è un campo intermedio. Mostriamo pertanto che $\mathrm{Gal}(E/L) = H$. Ovviamente $H \subseteq \mathrm{Gal}(E/L)$, mentre per vedere l'altra inclusione consideriamo separatamente i casi:

- H aperto. Allora, per la Proposizione 3.26, H è preimmagine di $H_M \subseteq \mathrm{Gal}(M/F)$ per un certo M finito e di Galois su F, quindi H coincide con l'insieme degli elementi di $\mathrm{Gal}(E/F)$ che ristretti a M sono in H_M. Sia ora $\sigma \in \mathrm{Gal}(E/E^H)$. Allora σ fissa tutti gli elementi di M^{H_M}, dal momento che dalla definizione risulta chiaro che $M^{H_M} \subseteq E^H$. Allora $\sigma \in \mathrm{Gal}(E/E^H) \subseteq \mathrm{Gal}(E/M^{H_M})$ e per il teorema di corrispondenza nel caso finito $\sigma_{|_M} \in \mathrm{Gal}(M/M^{H_M}) = H_M$, e pertanto $\sigma \in H$.

- H chiuso, ma non necessariamente aperto. Allora, per la Proposizione 3.24, esiste una famiglia $\mathcal{H}$ di sottogruppi aperti di G tale che $H = \bigcap \mathcal{H}$. Per ogni $U \in \mathcal{H}$ si ha $H \subseteq U$, pertanto $E^U \subseteq E^H = L$, da cui segue $\mathrm{Gal}(E/M) \subseteq \mathrm{Gal}(E/E^U)$. Possiamo allora concludere che

$$\mathrm{Gal}(E/L) \subseteq \bigcap_{U \in \mathcal{H}} \mathrm{Gal}(E/E^U) = \bigcap_{U \in \mathcal{H}} U = H.$$

Mostriamo ora che l'estensione L/F è di Galois se e solo se H è normale in G. Sia dapprima L/F di Galois e consideriamo $H := \mathrm{Gal}(E/L)$; siano $\tau \in H$, $\sigma \in G$ e proviamo che $\sigma^{-1}\tau\sigma \in H$, equivalentemente $(\sigma^{-1}\tau\sigma)(\alpha) = \alpha$ per ogni $\alpha \in L$. Per il Lemma 1.17 vale $\sigma(\alpha) \in L$ per ogni $\alpha \in L$, per cui

$$\begin{aligned}(\sigma^{-1}\tau\sigma)(\alpha) &= (\sigma^{-1}\tau)(\sigma)(\alpha)) \\ &= \sigma^{-1}\tau(\sigma(\alpha)) \\ &= \sigma^{-1}(\sigma(\alpha)) \\ &= \alpha.\end{aligned}$$

Viceversa sia $H \subseteq G$ un sottogruppo normale di G e sia $L := E^H$. Proviamo che per ogni $\sigma \in G$ e per ogni $z \in L$ vale $\sigma(z) \in L$, da cui segue, per il Lemma 1.17, la tesi. Siano quindi $\sigma \in G, z \in L$ e sia inoltre τ un elemento qualunque di H. Per normalità di H si ha $(\sigma^{-1} \circ \tau \circ \sigma)(z) = z)$, da cui segue $(\tau \circ \sigma)(z) = \sigma(z)$, e quindi $\sigma(z) \in E^H = L$. Proviamo ora che sotto queste ipotesi sussiste un isomorfismo fra $\mathrm{Gal}(L/F)$ e G/H. Consideriamo la mappa

$$\begin{aligned}\psi : \mathrm{Gal}(E/F) &\longrightarrow \mathrm{Gal}(L/F) \\ \sigma &\longmapsto \sigma_{|_L}.\end{aligned}$$

Questa mappa è ben definita per il Lemma 1.17 ed è suriettiva per il Lemma 1.13. Osserviamo infine che $ker(\psi) = \{\sigma \in G : \sigma_{|_L} = id_L\} = \mathrm{Gal}(K/L) = H$.
Mostriamo infine che l'estensione L/F è finita se e solo se H è un sottogruppo aperto di G. Se L è un campo intermedio finito su F, allora, per quanto mostrato a inizio dimostrazione, $\mathrm{Gal}(E/L)$ è aperto in G. Viceversa, supponiamo H aperto. Allora, per la Proposizione 3.25 si ha che $ker(\pi_M) \subseteq H$ per qualche campo intermedio $F \subseteq M \subseteq E$ finito e di Galois su F. Dal momento che $H \supseteq ker(\pi_M) = \mathrm{Gal}(E/M)$ si ha $L = E^H \subseteq E^{ker(\pi_M)} = E^{\mathrm{Gal}(E/M)} = M$. Quindi l'estensione L/F è finita. □

In questo modo abbiamo provato che è possibile estendere il teorema fondamentale a estensioni di grado infinito. Osserviamo inoltre che se E/F è un estensione di Galois finita, allora la topologia di Krull su $\mathrm{Gal}(E/F)$ è discreta e pertanto ogni suo sottogruppo chiuso, quindi riotteniamo la corrispondenza originale fra campi intermedi e sottogruppi.

Osservazione 4.2. Dato un generico sottogruppo $H < G := \mathrm{Gal}(E/F)$ vale che

$$\mathrm{Gal}(E/E^H) = \overline{H}.$$

Sia infatti $H < G$ come in ipotesi, allora E^H è un campo intermedio dell'estensione E/F. Per il teorema di corrispondenza esiste allora un sottogruppo $N < G$ chiuso tale che $E^H = E^N$; vale inoltre $\mathrm{Gal}(E/E^H) = \mathrm{Gal}(E/E^N) = N$. Poiché $H \subseteq \mathrm{Gal}(E/E^H) = N$, e N è chiuso, necessariamente deve valere $H \subseteq \overline{H} \subseteq N$, ma allora

$$N = \mathrm{Gal}(E/E^H) \supseteq \mathrm{Gal}(E/E^{\overline{H}}) \supseteq \mathrm{Gal}(E/E^N) = N.$$

e per il teorema di corrispondenza sappiamo che $\mathrm{Gal}(E/E^{\overline{H}}) = \overline{H}$, da cui segue immediatamente $\overline{H} = N$.

4.2 Casi di applicazione

Ora che abbiamo caratterizzato il gruppo di Galois di un'estensione di Galois infinita e abbiamo provato il teorema di corrispondenza nella sua forma più generica, è naturale chiedersi se questo risultato sia effettivamente utile: potrebbe essere il caso che le estensioni di Galois di grado infinito si presentino raramente, e che quindi il loro studio sia, in un certo verso, poco proficuo. Mostreremo invece in questa sezione come sia facile imbattersi in estensioni di questo tipo, e pertanto come sia utile il lavoro svolto finora. Introdurremo di seguito i concetti di campo ordinato e campo reale chiuso, per giungere ad un risultato di Artin e Schreier, dal quale risulterà chiaro come le estensioni di Galois infinite siano abbastanza frequenti.

Definizione 4.3. Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Chiameremo un tale campo "ordinato" per il semplice fatto che possiamo definire su F una relazione d'ordine ponendo, per ogni $a, b \in F$ che $a \leq b \iff (b-a) \in P$. Possiamo dedurre di più riguardo i campi ordinati: è chiaro che se $a \leq b$, allora per ogni $c \in F$ si ha $a + c \leq b + c$ e $ap \leq bp$ per ogni $p \in P$, quindi per ogni $a \in F^\times$ vale $a^2 = (-a)^2 > 0$. Questo implica che se $\sum_{i=1}^n a_i^2 = 0$, con gli $a_i \in F$, allora ogni $a_i = 0$. In particolare se ogni $a_i = 1$ otteniamo immediatamente $\sum_{i=1}^n 1 \neq 0$, ovvero ogni campo ordinato deve avere caratteristica 0. Esempi classici di gruppi ordinati sono $\mathbb{R}$ e $\mathbb{Q}$.

Definizione 4.4. Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Esempi di campi reali chiusi sono $\mathbb{R}$ e $\overline{\mathbb{Q}} \cap \mathbb{R}$, e possiamo pensare a queste strutture algebriche come dei campi "quasi" algebricamente chiusi. Il prossimo teorema specifica in modo preciso quanto appena detto.

Teorema 4.5. *Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.*

Non riporteremo per intero la prova di tale fatto; per una dimostrazione completa si consulti [3]. Siamo ora pronti a enunciare un importante risultato dovuto ad Artin e Schreier, dal quale comprenderemo l'utilità del lavoro che abbiamo svolto finora. Come prima, una possibile dimostrazione è reperibile in [3].

Teorema 4.6. *Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.*

Discutiamo ora l'utilità che il teorema 4.6 ha per noi: consideriamo un campo F, e sia $\overline{F}$ la sua chiusura algebrica, vediamo che se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$. Viceversa se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$. Ovviamente esistono moltissimi campi che non sono reali chiusi: $\mathbb{Q}$, $\mathbb{F}_p$ e $\mathbb{C}(x)$ sono solo alcuni di questi. Osserviamo inoltre che, per quanto noto dalla teoria elementare dei campi, ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile, pertanto quando il campo F che stiamo considerando ricade in una di queste due categorie, l'estensione $\overline{F}/F$ è separabile, ovviamente normale dal momento che $\overline{F}$ contiene le radici di ogni polinomio $f(Y) \in F[Y]$, e quindi è di Galois. Concludiamo quindi che la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è abbastanza utile, poiché la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Chiaramente non sempre accade che un estensione $\overline{F}/F$ sia di Galois, come mostra il seguente esempio:

Esempio 4.7. Sia $F := \mathbb{F}_2(t)$, dove t è un numero trascendente. Allora $\sqrt{t} \in \overline{F}$ poiché $\sqrt{t}$ è radice del polinomio $Y^2 - t \in F[Y]$, ma $Y^2 - t = (y - \sqrt{t})^2$ non è separabile, quindi $\overline{F}/F$ non è separabile, e pertanto neanche di Galois.

4.3 Gruppo di Galois assoluto

Scopo di questa sezione è descrivere il gruppo di Galois assoluto, un particolare tipo di gruppo di Galois per un'estensione di Galois infinita, molto utile nella pratica.

Definizione 4.8. Sia K/F un'estensione di campi. La chiusura separabile di F in K, denotata con F_{sep}, coincide con l'insieme $\{x \in K : x \text{ è separabile su } F\}$. Quando scriveremo F_{sep} senza indicare l'estensione di campi K di F, intenderemo sempre la chiusura separabile di F in $\overline{F}$.

Definizione 4.9. Sia K/F un'estensione di campi. Un elemento $\alpha \in K$ è inseparabile su F se il polinomio minimo f di α su F ha almeno una radice doppia. Diremo che α è puramente inseparabile su F se f ha solamente α come radice. L'estensione K/F si dice puramente inseparabile se ogni $\alpha \in K$ è puramente inseparabile.

Si verifica facilmente che F_{sep} è in realtà un campo, inoltre, come detto prima, ogni estensione algebrica di un campo finito o di caratteristica p è separabile, pertanto un'estensione non separabile la possiamo ottenere solamente partendo da un campo di caratteristica $p > 0$; segue ovviamente che ogni estensione puramente inseparabile ha caratteristica un primo p.

Osservazione 4.10. Non è difficile provare che se E/F è un'estensione di campi di caratteristica $p > 0$, e $\alpha \in E$ è inseparabile su F, allora esiste un minimo n naturale positivo e un polinomio $g \in F[Y]$ inseparabile e irriducibile su F tale che , posto f il polinomio minimo di α su F, si abbia $f(x) = g(x^{p^n})$. Questo fatto ci è utile nel provare la seguente proposizione.

Proposizione 4.11. *Siano F un campo di caratteristica un primo p e K/F un'estensione algebrica; poniamo F_{sep} la chiusura separabile di F in K. Allora l'estensione K/F_{sep} è puramente inseparabile.*

Dimostrazione. Sia $\alpha \in F_{sep}$, allora il polinomio minimo di α su F_{sep} è $f := Y - \alpha$, che è chiaramente puramente inseparabile. Consideriamo quindi $\alpha \in K \setminus F_{sep}$ e poniamo $f \in F_{sep}[Y]$ il polinomio minimo di α su F_{sep}. Per quanto visto con l'osservazione precedente esiste un naturale positivo n ed esiste $g \in F_{sep}[Y]$ separabile e irriducibile tale che $f(Y) = g(Y^{p^n})$. Poniamo $a := \alpha^{p^n}$, allora $g(a) = f(\alpha) = 0$, ma poiché g è irriducibile abbiamo che g è il polinomio minimo di a su F_{sep}. Siccome g è separabile otteniamo $a \in F_{sep}$, e quindi $f = Y^{p^n} - a = (x - \alpha)^{p^n}$, dove per l'ultima uguaglianza abbiamo usato il fatto che E ha caratteristica p, quindi α è puramente inseparabile su F_{sep}, come richiesto. □

Proposizione 4.12. *Sia F un campo di caratteristica p, $\overline{F}$ la sua chiusura algebrica, e F_{sep} la sua chiusura separabile in $\overline{F}$. Allora F_{sep}/F è di Galois e $Gal(\overline{F}/F) \cong Gal(F_{sep}/F)$.*

Dimostrazione. Sia $\alpha \in F_{sep}$, allora il polinomio minimo f di α su F ha tutte radici distinte, pertanto se β è una seconda radice di f, necessariamente $\beta \in F_{sep}$. Questo implica che F_{sep}/F è un'estensione normale. Quindi F_{sep}/F è di Galois.
Consideriamo ora la mappa

$$\begin{aligned} \theta \colon \mathrm{Gal}(\overline{F}/F) &\longrightarrow \mathrm{Gal}(F_{sep}/F) \\ \sigma &\longmapsto \sigma_{|_{F_{sep}}}. \end{aligned}$$

Si verifica che è un omomorfismo di gruppi ben definito, e $\ker(\theta) = \mathrm{Gal}(\overline{F}/F_{sep})$. Mostriamo che $\ker(\theta) = \{1\}$, da cui segue immediatamente la tesi. Sia $\alpha \in \overline{F}$ e sia $\tau \in \mathrm{Gal}(\overline{F}/F_{sep})$. $\tau(\alpha)$ è allora una radice di f, il polinomio minimo di α su F_{sep}, tuttavia dalla Proposizione 4.11 si ha che α è puramente inseparabile su F_{sep}, pertanto f ha un'unica radice α (contata senza molteplicità ovviamente). Concludiamo che $\tau(\alpha) = \alpha$ per ogni $\alpha \in \overline{F}$, e quindi $\ker(\theta) = 1$. □

Definizione 4.13. Il gruppo $G := \mathrm{Gal}(F_{sep}/F)$ è detto gruppo di Galois assoluto del campo F.

Osserviamo che, nel caso in cui il campo di base F sia finito oppure di caratteristica zero, il gruppo di Galois assoluto di F coincide con $\mathrm{Gal}(\overline{F}/F)$.

4.4 Esempi

In questa sezione porremo l'attenzione sul gruppo di Galois assoluto di $\mathbb{F}_p$ per un certo primo p. Come abbiamo avuto modo di notare prima, poiché $\mathbb{F}_p$ è un campo finito, ogni sua estensione algebrica è anche separabile, pertanto il gruppo di Galois assoluto di $\mathbb{F}_p$ coincide con $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Avremo bisogno di alcuni risultati tecnici preliminari.

Teorema 4.14. *Per ogni primo p e ogni intero $n \geq 1$ esiste un campo finito con p^n elementi. Ogni campo finito con p^n elementi è isomorfo al campo di spezzamento del polinomio $Y^{p^n} - Y \in \mathbb{F}_p[Y]$.*

Il teorema appena enunciato mostra che, dato $q = p^n$, esiste un unico campo finito con p^n elementi. Denotiamo tale campo come $\mathbb{F}_q$ e lo chiameremo *il* campo finito con q elementi. Si ha inoltre che tale campo coincide con il campo di spezzamento del polinomio $Y^q - Y$ su $\mathbb{F}_p$, e pertanto $\mathbb{F}_q/\mathbb{F}_p$ è un'estensione di Galois di grado n. Mostriamo ora qualche risultato in più riguardo la struttura di $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Lemma 4.15. *Il gruppo di Galois $Gal(\mathbb{F}_q/\mathbb{F}_p)$, con $q = p^n$ è un gruppo ciclico di ordine n generato dal morfismo di Frobenius.*

Dimostrazione. È chiaro che il morfismo di Frobenius $\phi : \alpha \mapsto \alpha^p$ è un elemento di $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Osserviamo che il gruppo di Galois di tale estensione è finito, dal momento che $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$. Possiamo quindi considerare $m \in \{1, ..., n\}$ tale che $\phi^m \equiv 1$. Allora $\phi^m(\alpha) = \alpha$, e cioè $\alpha^{p^m} - \alpha = 0$ per ogni $\alpha \in \mathbb{F}_p$. Segue che il polinomio $Y^{p^m} - Y$ ha almeno $q = p^n$ radici. Quindi $p^m \geq p^n$, ovvero $m \geq n$. Necessariamente deve valere $m = n$. □

Lemma 4.16. *Il campo $\mathbb{F}_{p^m}$ è un sottocampo di $\mathbb{F}_{p^n}$ se e solo se m divide n.*

Dimostrazione. Se $m|n$, allora esiste un sottogruppo $H < \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ con $|H| = n/m$, dal momento che $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ è un gruppo ciclico di ordine n per il Lemma 4.15. Sia M il sottocampo di $\mathbb{F}_{p^n}/\mathbb{F}_p$ fissato da H. Sappiamo che $[M : \mathbb{F}_p] = m$, pertanto $M = \mathbb{F}_{p^m}$, per l'unicità dei campi finiti. Viceversa, sia $\mathbb{F}_{p^m}$ un sottocampo di $\mathbb{F}_{p^n}$. Allora il grado $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$ divide il grado $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$. □

Teorema 4.17. *Sia q una potenza di un primo. Allora valgono i seguenti fatti:*

(*i*) *$\mathbb{F}_q$ è un sottocampo di $\mathbb{F}_{q^n}$ per ogni $n \geq 1$.*

(*ii*) *$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ è un gruppo ciclico di ordine n generato dal morfismo di Frobenius.*

(*iii*) *$\mathbb{F}_{q^m}$ è un sottocampo di $\mathbb{F}_{q^n}$ se e solo se m divide n.*

Dimostrazione.

(*i*) Sia $q = p^s$ per qualche primo p e qualche $s \geq 1$, allora per il Lemma 4.16 si ha che $\mathbb{F}_q = \mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^{ns}} = \mathbb{F}_{q^n}$.

(*ii*) Si procede in maniera analoga a come fatto con il Lemma 4.15, semplicemente sostituendo p con q.

(*iii*) Per il Lemma 4.16, $\mathbb{F}_{q^m} = \mathbb{F}_{p^{ms}}$ è un sottocampo di di $\mathbb{F}_{q^m} = \mathbb{F}_{p^{ns}}$ se e solo se ms divide ns. Questo è equivalente a chiedere che m divida n.

□

Teorema 4.18. *La chiusura algebrica di $\mathbb{F}_q$ coincide con l'unione $\cup_{n=1}^{\infty}\mathbb{F}_{q^n}$*

Dimostrazione. Denotiamo con $U := \cup_{n=1}^{\infty}\mathbb{F}_{q^n}$. È immediato osservare che $U \subseteq \overline{\mathbb{F}}_p$, dal momento che se $x \in U$, allora esiste $n \in \mathbb{N}$ tale che $x \in \mathbb{F}_{q^n}$, ma $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n < \infty$, e pertanto x è algebrico su $\mathbb{F}_q$. Si mostra altrettanto facilmente che U è un campo. Mostriamo che U è algebricamente chiuso, da cui seguirà l'asserto. Consideriamo $f(Y) := \sum_{i=0}^{s} \lambda_i Y^i \in U[Y]$ un polinomio non costante. Per ogni $i \in \{0, ..., s\}$ si ha che $\lambda_i \in \mathbb{F}_{q^{m_i}}$, per qualche $m_i \geq 1$. Di conseguenza, per il Teorema 4.17(*iii*), $f(Y)$ è un polinomio a coefficienti in $\mathbb{F}_{q^m}$, dove $m := \prod_{i=0}^{s} m_i$. Sia α una radice di f. Allora $\mathbb{F}_{q^m}(\alpha)$ è un'estensione algebrica di $\mathbb{F}_{q^m}$ e $\mathbb{F}_{q^m}(\alpha)$ può essere visto come spazio vettoriale finito-dimensionale su $\mathbb{F}_{q^m}$. D'altronde $\mathbb{F}_{q^m}(\alpha)$ è un campo finito contenente $\mathbb{F}_q$. Sia r il grado di tale estensione, allora $\mathbb{F}_{q^m}(\alpha)$ contiene esattamente q^{rm} elementi, ovvero $\mathbb{F}_{q^m}(\alpha) = \mathbb{F}_{q^{rm}}$. Quindi α è un elemento di U, ed è algebrico su $\mathbb{F}_{q^m}$. □

Osservazione 4.19. Tenedo presente quando appena visto e quanto invece mostrato con l'Esempio 3.16 è immediato concludere che la chiusura algebrica di un campo con un numero primo di elementi è un esempio di limite diretto.

Osservazione 4.20. Come abbiamo avuto modo di osservare con l'Esempio 3.4, possiamo considerare $\mathbb{N}$ e la relazione $R \subseteq \mathbb{N}\times\mathbb{N}$ definita ponendo $(m,n) \in R \Leftrightarrow m|n$. Consideriamo inoltre la famiglia di gruppi $\{G_n := \mathbb{Z}/n\mathbb{Z}\}$ indicizzata su $n \in \mathbb{N}$ e per ogni $(n,m) \in R$ siano $\varphi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la mappa tale che $a+m\mathbb{Z} \mapsto a+n\mathbb{Z}$, e φ_{nn} la mappa identica. Allora si verifica facilmente che $\{\mathbb{Z}/n\mathbb{Z}, \varphi_{nm}\}$ costituisce un sistema inverso di gruppi. Abbiamo denotato il limite inverso $\varprojlim \mathbb{Z}/n\mathbb{Z}$ di tale sistema con $\hat{\mathbb{Z}}$.

Possiamo caratterizzare in termini insiemistici $\hat{\mathbb{Z}}$; a tal proposito enunciamo la seguente proposizione.

Proposizione 4.21. *Se poniamo $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, ovvero l'insieme delle successioni coerenti in $\mathbb{Z}/p^n\mathbb{Z}$, allora $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.*

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} \varphi\colon \ \hat{\mathbb{Z}} &\longrightarrow \textstyle\prod_p \mathbb{Z}_p \\ \{\sigma_n\} &\longmapsto \{\{\sigma_{p^n}\}_n\}_p. \end{aligned}$$

Osserviamo che tale mappa è ben definita, poiché successioni coerenti vengono mappate in successioni coerenti. Mostriamo che φ è iniettiva: consideriamo un elemento $\{\sigma_n\}_n$ tale che $\varphi(\{\sigma_n\}) = \{\{0\}\}$, ovvero tale che $\sigma_{p^n} \equiv 0$ per ogni $n \in \mathbb{N}$ e per ogni p primo. Mostriamo che $\sigma_m \equiv 0\ (m)$ per ogni $m \in \mathbb{N}$. Sia quindi $m = p_1^{e_1}\cdots p_r^{e_r}$ un naturale generico, allora per ipotesi $\sigma_{p_i^{e_i}} \equiv 0$ per ogni i. Dovendo inoltre naturalmente valere $\sigma_m \equiv \sigma_{p_i^{e_i}} \equiv 0\ (p_i^{e_i})$ per ogni $i \in \{1,...,r\}$, allora per il teorema cinese $\sigma_m \equiv 0\ (m)$. Mostriamo ora che φ è suriettiva: sia $\{\{\sigma_{p^n}\}_n\}_p$ un generico elemento di $\prod_p \mathbb{Z}_p$. È sufficiente provare che esiste $\{\overline{\sigma_n}\}$ tale che, se $n = p_1^{e_1}\cdots p_r^{e_r}$, allora $\overline{\sigma_n} \equiv \sigma_{p_i^{e_i}}\ (p_i^{e_i})$ per ogni i. Tale sistema ha soluzione per il teorema cinese, e si può verificare che tale soluzione è coerente. □

Gli elementi di $\hat{\mathbb{Z}}$ prendono il nome di interi profiniti, e si possono ottenere come completamento profinito del gruppo $\mathbb{Z}$; mostriamo formalmente quanto detto. Ricordiamo innanzitutto che dato un arbitrario gruppo G, possiamo sempre associargli un gruppo profinito, che chiameremo completamento profinito di G. Questo è definito come il limite inverso della famiglia di gruppi G/N, dove N descrive un generico sottogruppo normale di G di indice finito (questi sottogruppi normali sono parzialmente ordinati dall'inclusione, il che si traduce in un sistema inverso in cui i morfismi sono quelli naturali fra i quozienti). Dal momento che i sottogruppi di indice finito di $\mathbb{Z}$ sono tutti del tipo $\mathbb{Z}/n\mathbb{Z}$, allora, poiché $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, possiamo affermare che il gruppo degli interi profiniti coincide con il completamento profinito di $\mathbb{Z}$.

Osservazione 4.22. Consideriamo $\mathbb{F}_q$ il campo finito con q elementi, e consideriamo la famiglia di gruppi $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, per ogni $n \in \mathbb{N}$. Abbiamo avuto modo di osservare che $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ se e solo se $m|n$. Consideriamo la relazione R definita ponendo $(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)) \in R$ se e solo se $m|n$. In tal caso, poiché $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ possiamo definire un morfismo

$$\begin{aligned} \varphi_{mn}\colon \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) &\longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ \sigma &\longmapsto \sigma_{|_{\mathbb{F}_{q^n}}}. \end{aligned}$$

Allora $\{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \varphi_{mn}\}$ formano un sistema inverso di gruppi indicizzato su $\mathbb{N}$.

Teorema 4.23. *Gal*$(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim$ *Gal*$(\mathbb{F}_{q^n}/\mathbb{F}_q)$

Dimostrazione. Per ogni $n \in N$ abbiamo un omomorfismo $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ ottenuto tramite la restrizione di un elemento generico in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Questi omomorfismi, nel loro complesso, generano un omomorfismo

$$\begin{aligned} \theta\colon \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) &\longrightarrow \textstyle\prod_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ \sigma &\longmapsto \{\sigma_{|_{\mathbb{F}_{q^n}}}\}_{n\in\mathbb{N}}. \end{aligned}$$

È immediato verificare che l'immagine di θ sia contenuta in $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Osserviamo che θ è iniettiva, dal momento che se $\sigma \neq 1$ è un elemento di $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, allora esiste un elemento $x \in \overline{\mathbb{F}_q}$ tale che $\sigma(x) \neq x$. Per il teorema 4.18 x appartiene a $\mathbb{F}_{q^m}$, per qualche $m \in \mathbb{N}$. Allora l'immagine di σ in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ mappa x in $\sigma(x) \neq x$. Concludiamo che $\theta(\sigma)$ non coincide con l'identità di $\prod_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Proviamo infine che l'immagine di θ è proprio $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Sia $(\sigma_n) \in \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Definiamo una mappa $\sigma : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$ nel seguente modo: se $x \in \overline{\mathbb{F}_q}$, allora $\sigma(x) = \sigma_m(x)$, qualora $x \in \mathbb{F}_{q^m}$. Tale mappa è ben definita e costituisce un elemento di $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Dal momento che per costruzione $\theta(\sigma) = (\sigma)_n$, l'asserto risulta provato. □

Corollario 4.24. *Gal*$(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$

Dimostrazione. Per ogni $n \in \mathbb{N}$, per il Teorema 4.17 possiamo identificare il gruppo di Galois $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ con $\mathbb{Z}/n\mathbb{Z}$. Abbiamo in questo modo provato che il seguente diagramma commuta

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) & \xrightarrow{\phi_{mn}} & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \end{array}$$

da cui segue immediatamente che $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$ □

Osservazione 4.25. Soffermiamoci a discutere alcuni dettagli dell'estensione $\overline{\mathbb{F}_p}/\mathbb{F}_p$, in particolare il rapporto che il morfismo di Frobenius ha con il gruppo di Galois di tale estensione. Osserviamo innanzitutto che $G := \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ è tale che $\overline{\mathbb{F}_p}^G = \mathbb{F}_p$. Sia ϕ il morfismo di Frobenius di $\overline{\mathbb{F}_p}$, allora $\langle\phi\rangle < G$ e vale che $\overline{\mathbb{F}_p}^{\langle\phi\rangle} = \mathbb{F}_p$. Per quanto visto con l'Osservazione 4.2 si ottiene immediatamente che $\overline{\langle\phi\rangle} = G$. Non avremmo potuto ottenere lo stesso risultato se avessimo considerato solamente $\langle\phi\rangle$, dal momento che $\langle\phi\rangle \lneq G$. Proviamo tale fatto: poiché $\langle\phi\rangle \cong \mathbb{Z}$, tutti i suoi sottogruppi hanno indice finito; se per assurdo fosse $\langle\phi\rangle = G$, allora ogni sottocampo proprio F di $\overline{\mathbb{F}_p}/\mathbb{F}_p$ avrebbe grado finito $|F : \mathbb{F}_p|$. Questo non può succedere, dal momento che $F := \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{2^n}}$ è un campo intermedio tale che la dimensione $|F : \mathbb{F}_p|$ è infinita. Concludiamo che considerare la chiusura del sottogruppo $\langle\phi\rangle$ è essenziale e irrinunciabile.

Esempio 4.26. Supponiamo ora di voler trovare tutte le sottoestensioni di $\overline{\mathbb{F}}_p/\mathbb{F}$, o equivalentemente tutti i sottogruppi chiusi di $\hat{\mathbb{Z}}$.
Sia q un primo, e denotiamo con $L_q := \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{q^n}}$. Si verifica facilmente che:

- L_q è unione di estensioni concentriche;
- $|L_q : \mathbb{F}_p| = \infty = |\overline{\mathbb{F}}_p : L_q|$;

- $\mathrm{Gal}(L_q : \mathbb{F}_p) \cong \mathbb{Z}_q$;

Sia $\mathbb{F}_p \subseteq F \subseteq L_q$ un campo intermedio e sia $q^{n_F} := \sup_{x\in F}\{|\mathbb{F}_p(x) : \mathbb{F}_p|\}$, con $0 \leq n_F \leq \infty$. Proviamo allora che $F = \mathbb{F}_{p^{q^{n_F}}}$.

- $\subseteq$ Se $n_F = \infty$ allora l'inclusione è ovvia. Supponiamo quindi $n_F < \infty$; sia $x \in F$, allora $|\mathbb{F}_p(x) : \mathbb{F}_p| \leq q^{n_F}$, ma per come abbiamo costruito L_q si ha $|\mathbb{F}_p(x) : \mathbb{F}_p| \mid q^{n_F}$, e ricordando il Lemma 4.16 si ottiene che $\mathbb{F}_p(x) \subseteq \mathbb{F}_{p^{q^{n_F}}}$.

- $\supseteq$ Se $n_F = \infty$ allora esistono elementi di grado arbitrariamente grande su $\mathbb{F}_p$, ma per ogni $x \in \mathbb{F}_{p^{q^n}}$ la dimensione $|\mathbb{F}_p(x) : \mathbb{F}_p|$ è finita; per come abbiamo costruito l'estensione L_q segue che $\mathbb{F}_{p^{q^n}} \subseteq F$. Supponiamo quindi $n_F < \infty$, allora esiste $x \in F$ tale che $|\mathbb{F}_p(x) : \mathbb{F}_p| = q^{n_F}$ e pertanto $\mathbb{F}_{p^{q^{n_F}}} = \mathbb{F}_p(x)$

Per il teorema di corrispondenza in dimensione infinita deduciamo quindi che i sottogruppi chiusi di $\mathbb{Z}_q$ sono tutti e soli gli elementi del tipo $\mathrm{Gal}(L_q/\mathbb{F}_{p^{q^n}})$, al variare di $n \in \mathbb{N}\cup\{\infty\}$. Proviamo ora che i sottogruppi chiusi di $\mathbb{Z}_q$ sono della forma $q^n\mathbb{Z}_q$. Sia ϕ il morfismo di Frobenius di $L_q/\mathbb{F}_p$, allora, per quando visto prima, si ha $\mathbb{Z}_q \cong \mathrm{Gal}(L_q/\mathbb{F}_p) \cong \overline{\langle\phi\rangle}$. Osserviamo che per lo stesso motivo $\mathrm{Gal}(L_q/\mathbb{F}_{p^{q^m}}) \cong \overline{\langle\phi^{q^m}\rangle}$, ma se consideriamo l'isomorfismo

$$\begin{aligned}\varphi\colon \overline{\langle\phi\rangle} &\longrightarrow \mathbb{Z}_q\\ \phi &\longmapsto 1\end{aligned}$$

che lega $\overline{\langle\phi\rangle}$ e $\mathrm{Gal}(L_q/\mathbb{F}_p)$. Abbiamo indicato con $1 := \{\left[1\right]_{q^n}\}_{n\in\mathbb{N}}$. Si ha in particolare che la restrizione

$$\begin{aligned}\varphi_{|_{\overline{\langle\phi^{q^m}\rangle}}}\colon \overline{\langle\phi^{q^m}\rangle} &\longrightarrow q^m\mathbb{Z}_q\\ \phi^{q^m} &\longmapsto q^m\end{aligned}$$

definisce un isomorfismo fra $\overline{\langle\phi^{q^m}\rangle}$ e $q^m\mathbb{Z}_q$. Ancora abbiamo identificato $q^m := \{\left[q^m\right]_{q^n}\}_{n\in\mathbb{N}}$. Concludiamo quindi che i sottogruppi chiusi di $\mathbb{Z}_q$ sono della forma $q^m\mathbb{Z}_q$, per qualche $m \in \mathbb{N}\cup\{\infty\}$. Passiamo ora al caso generale di un'estensione intermedia K di $\overline{\mathbb{F}}_p/\mathbb{F}_p$. Preso un qualunque primo q, denotiamo $K^{(q)} := K \cap L_q$. Proviamo che vale

$$K = \prod_q K^{(q)},$$

dove abbiamo indicato con $\prod_q K^{(q)}$ il più piccolo sottocampo di $\overline{\mathbb{F}_p}$ che contiene ogni $K^{(q)}$.

- $\subseteq$ Sia $x \in K$, e diciamo che $|\mathbb{F}_p(x) : \mathbb{F}_p| = m$, con $m = q_1^{e_1}\cdot\cdots\cdot q_r^{e_r}$; allora per il teorema cinese del resto otteniamo che $x \in \mathbb{F}_{p^m} = \prod_i \mathbb{F}_{p^{q_i^{e_i}}} \subseteq \prod_i K^{(q_i)}$.

- $\supseteq$ Ovviamente, in quanto ciascuno dei $K^{(q)}$ è contenuto in K.

Per quanto visto prima si ha che $K^{(q)} = \mathbb{F}_{p^{q^{n_q}}}$, per qualche $n_q \in \mathbb{N}\cup\{\infty\}$, da cui segue

$$K = \prod_q \mathbb{F}_{p^{q^{n_q}}}.$$

Per ogni q consideriamo il morfismo $\theta : \mathrm{Gal}(\overline{\mathbb{F}_p}/K) \to \mathrm{Gal}(L_q/K^{(q)})$ tale che $\sigma \mapsto \sigma_{|_{L_q}}$. Osserviamo che la scelta del codominio non è sbagliata, dal momento che se σ è un elemento

di $\mathrm{Gal}(\overline{\mathbb{F}_p}/K) \subseteq \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F})$, allora $\sigma_{|_{L_q}} \in \mathrm{Gal}(L_q/\mathbb{F})$ ed è quindi un automorfismo di L_q che chiaramente fissa $K^{(q)}$. Tali mappe generano un ulteriore morfismo

$$\begin{aligned} \theta\colon \mathrm{Gal}(\overline{\mathbb{F}_p}/K) &\longrightarrow \textstyle\prod_q \mathrm{Gal}(L_q/K^{(q)}) \\ \sigma &\longmapsto \sigma_{|_{L_q}}. \end{aligned}$$

Ma le estensioni $K^{(q)} = \mathbb{F}_{p^{q^{n_q}}}$ hanno a due a due intersezione banale, ovvero $\mathbb{F}_p$, e grazie a questo si verifica facilmente che θ è un morfismo biiettivo, ovvero

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/K) \cong \prod_q \mathrm{Gal}(L_q/K^{(q)}) \cong \prod_q q^{n_q}\mathbb{Z}_q.$$

Concludiamo che i sottogruppi chiusi di $\hat{\mathbb{Z}}$ sono quelli del tipo $\prod_q q^{n_q}\mathbb{Z}_q$, al variare di $n_q \in \mathbb{N} \cup \{\infty\}$.

Bibliografia

[1] Serena Cicalò, Willem A. de Graaf. *Teoria di Galois*. Aracne editrice, Roma, 2008.

[2] P. J. Higgins. *An Introduction to Topological Groups*. Cambridge University Press, New York, 1975.

[3] Nathan Jacobson. *Basic Algebra II*. W.H. Freeman and Co., New York, 1989.

[4] Irving Kaplansky. *Fields and rings*. University of Chicago Press, Chicago, 1972.

[5] Serge Lang. Algebra. Addison-Wesley Publishing Co., Melino Park CA, 1984.

[6] Tamás Szamuely. *Galois groups and fundamental groups*. Cambridge University Press, 2009.