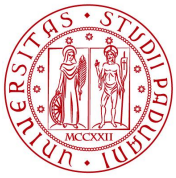

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Estensioni Trascendenti

Relatore:
Prof. Riccardo Colpi

Laureando: Alessandro Giuriati
Matricola: 2003226

Anno Accademico 2023/2024

23/02/2024

Indice

Introduzione

Alla base di questo studio vi è l'analisi delle estensioni trascendenti di campi, della loro struttura e delle loro proprietà con particolare riguardo alle loro applicazioni all'interno della teoria di Galois.

Il primo capitolo è introduttivo: si richiamano alcune nozioni nell'ambito della teoria dei campi tra cui la definizione di elemento algebrico e di elemento trascendente. Un primo approccio storico di quest'ultimi risale alla seconda metà del diciannovesimo secolo per opera di importanti matematici come Jospeh Liouville (1809-1882), Charles Hermite (1822-1901), Ferdinand von Lindemann (1852-1939) e George Cantor (1845-1918) che contribuirono allo studio e all'approfondimento dei numeri trascendenti.

Nel secondo capitolo si introducono le nozioni di dipendenza ed indipendenza algebrica e delle proprietà che costituiscono la base dello studio delle estensioni trascendenti. In particolare viene trattata la nozione di estensione puramente trascendente per poter introdurre il concetto di base di trascendenza, nozione fondamentale per la caratterizzazione delle estensioni trascendenti. Infine si dimostra il Teorema di Lüroth che risolve in un caso specifico il problema di determinare se un'estensione finitamente generata sia puramente trascendente o meno.

Il terzo capitolo è dedicato allo studio della teoria di Galois per estensioni algebriche non necessariamente finite. Richard Dedekind provò che nel caso infinito viene a mancare la corrispondenza biunivoca tra i sottogruppi del gruppo di Galois e i campi intermedi di un'estensione, e Wolfgang Krull (1899-1971) risolse il problema dotando il gruppo di Galois di una topologia che prese il nome di Topologia di Krull.

L'ultimo capitolo estende ulteriormente la teoria di Galois al caso di estensioni non necessariamente algebriche. Seguendo il lavoro [6], si introdurrà una topologia $\mathcal{T}$, che chiameremo di Soundararajan e Venkatachaliengar, che consente di stabilire in questo contesto più generale un risultato analogo a quello trattato nel capitolo precedente.

Capitolo 1

Estensioni

In questo capitolo introduttivo ricordiamo alcune nozioni preliminari nell'ambito della teoria dei campi, con particolare riguardo ai concetti di elementi algebrici ed elementi trascendenti.

1.1 Estensioni di Campi

Definizione 1.1 (Estensione di Campi)**.** Sia K un campo. Un'*Estensione* di K è un campo Ω che continene K come sottocampo. In particolare Ω è in modo naturale un K-spazio vettoriale la cui dimensione è per definizione il grado $[\Omega : K]$ di Ω su K. Un'estensione si dice finita se il suo grado è finito.

Useremo il simbolo Ω/K per denotare che Ω è un'estensione di K.

Proposizione 1.1. Consideriamo i campi $K \leq L \leq \Omega$. Allora Ω/K ha grado finito se e solo se Ω/L e L/K hanno entrambi grado finito, e in tal caso vale l'identità

$$[\Omega : K] = [\Omega : L][L : K]$$

Dimostrazione. Se Ω è finito su K, allora Ω è certamente finito su L; inoltre L, diventando un sottospazio di un K-spazio vettoriale di dimensione finita, è finito. Assumiamo ora che Ω/L e L/K abbiano grado finito e sia $(e_i)_{1\leq i\leq m}$ una base per L come K-spazio vettoriale e $(l_j)_{1\leq j\leq n}$ una base per Ω come L-spazio vettoriale. Completeremo la dimostrazione provando che $(e_i l_j)_{1\leq i\leq m, 1\leq j\leq n}$ è una base per Ω su K:

I) $(e_i l_j)_{i,j}$ generano Ω: Sia $\gamma \in L$. Poichè $(l_j)_j$ è base di Ω come L-spazio vettoriale,

$$\gamma = \sum_{j=1}^{n} a_j l_j, \qquad a_j \in L$$

e poichè $(e_i)_i$ è base di L come K-spazio vettoriale,

$$a_j = \sum_{i=1}^{m} a_{ij} e_i, \qquad a_{ij} \in K.$$

Dunque troviamo

$$\gamma = \sum_{i,j} a_{ij} e_i l_j.$$

II) $(e_i l_j)_{i,j}$ sono linearmente indipendenti: sia $\sum a_{ij} e_i l_j = 0$ con $a_{ij} \in K$, allora la sommatoria può essere riscritta come $\sum_j (\sum_i a_{ij} e_i) l_j = 0$. Ma l'indipendenza lineare degli l_j mostra che $\sum_i a_{ij} e_i = 0 \ \forall j$, e l'indipendenza lineare degli e_i mostra che $a_{ij} = 0$. □

Definizione 1.2 (Estensioni generate ed estensioni semplici)**.** Sia Ω/K un'estensione e $A \subseteq \Omega$. Denotiamo con $K(A)$ l'intersezione di tutti i sottocampi di Ω che contengono K ed A. Chiaramente $L/K(A)$ e $K(A)/K$ sono estensioni; $K(A)/K$ è detta l'estensione di K *generata da* A. Se $A = \{\alpha_1, \ldots, \alpha_n\}$, scriviamo $K(\alpha_1, \ldots, \alpha_n)$ per $K(A)$. Un'estensione Ω/K è *semplice* se esiste $\alpha \in L$ tale che $\Omega = K(\alpha)$.

Sia Ω/K. Un elemento $\alpha \in \Omega$ definisce un omomorfismo di anelli chiamato *valutazione di* α:

$$\nu_\alpha : K[x] \to \Omega, \ f(x) \mapsto f(\alpha)$$

Osservazione: $Im(\nu_\alpha) = K[\alpha]$ è il minimo sottoanello di Ω contenente K e α.
Ci sono due possibilità:

- CASO I: Il Kernel della mappa è $\neq (0)$, cioè esiste un $g(x) \in K[x]$, $g \neq 0$ tale che $g(\alpha) = 0$. In questo caso diciamo che α è *algebrico* su K. Ora l'ideale $Ker(\nu_\alpha)$ è costituito dai polinomi $g(x) \in K[x]$ tali che $g(\alpha) = 0$. Poiché $K[x]$ è un dominio ad ideali principali, si ha che $Ker(\nu_\alpha) = (f)$ per un unico polinomio monico $f \in K[x]$, detto *polinomio minimo* di α su K. Tale f è quindi il polinomio monico di minimo grado che sta in $Ker(\nu_\alpha)$. Così $K[x]/(f) \cong Im(\nu_\alpha) = K[\alpha] \leq \Omega$ è dominio, perciò (f) è primo e quindi massimale, e così $K[\alpha] = K(\alpha)$ è sottocampo di Ω. In particolare f è irriducibile.

- CASO II: Il Kernel della mappa è (0). Dunque per $f \in K[x]$,

  $$f(\alpha) = 0 \implies f = 0 \qquad (in\, K[x])$$

  In questo caso, diciamo che α è *trascendente* su K. L'omomorfismo $K[x] \to K[\alpha]$: $x \mapsto \alpha$ è un isomorfismo dato che $Ker(\nu_\alpha) = (0)$, e come tale si estende ai rispettivi campi di frazioni $K(x) \cong K(\alpha)$.

Cenni storici: Un numero complesso è detto *algebrico* o *trascendente* se esso è algebrico o trascendente su $\mathbb{Q}$. Nel 1844 Liouville dimostrò che un insieme di numeri, che ora chiamiamo *numeri di Liouville*, sono trascendenti. Nel 1873 Hermite mostrò che il numero di Nepero e è trascendente mentre nel 1882 Lindemann mostrò che π è trascendente. Nel 1874 Cantor provò che l'insieme dei numeri algebrici è numerabile cioè ha cardinalità $\aleph_0$, derivandone che la cardinalità degli elementi trascendenti, quella $2^{\aleph_0}$del continuo, è strettamente maggiore.

Capitolo 2

Estensioni trascendenti ed Indipendenza Algebrica

In questo capitolo introdurremo i concetti di indipendenza algebrica e di base di trascendenza. Concluderemo poi dimostrando un importante risultato che coinvolge una particolare tipologia di estensioni trascendenti.

2.1 Elementi trascendenti ed indipendenza algebrica

Definiamo gli elementi algebricamente indipendenti di un'estensione Ω/K. Siano $\alpha_1, \ldots, \alpha_n$ elementi di Ω. Analogamente a quanto introdotto nel primo capitolo, essi definiscono il K-omomorfismo di valutazione

$$\phi : K[x_1, \ldots, x_n] \to \Omega, \ f(x_1, \ldots, x_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$$

Se il $Ker(\phi) = (0)$, allora gli α_i sono detti *algebricamente indipendenti* su K. Quindi gli α_i sono algebricamente indipendenti se e solo se $\forall a_{i_1,\ldots,i_n} \in K$, se $\sum a_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} = 0$ allora tutti i coefficienti $a_{i_1,\ldots,i_n}$ sono nulli. Si noti come l'indipendenza algebrica di $\alpha_1, \ldots, \alpha_n$ sia analoga alla lineare indipendenza dei loro possibili prodotti $\alpha_1^{i_1} \cdots \alpha_n^{i_n}$.

Osservazioni: Un insieme vuoto è sempre algebricamente indipendente, mentre un singolo elemento α è algebricamente indipendente su K se e solo se è trascendente su K. Infine una lista di elementi $\{\alpha_1, \ldots, \alpha_n\}$ che contiene una ripetizione è algebricamente dipendente perchè se $\alpha_j = \alpha_k$ con $j \neq k$ allora il polinomio $f(x_1, \ldots, x_n) = x_j - x_k$ si annulla quando sostituiamo gli α_i agli x_i.

Un insieme inifinto A è detto *algebricamente indipendente* su K se ogni sottoinsieme finito di A risulta tale. Altrimenti esso è *algebricamente dipendente* su K.

Definizione 2.1. Sia Ω/K un'estensione di campi. Essa è detta *estensione algebrica* se ogni $\alpha \in \Omega$ è algebrico su K. In caso contrario è detta *estensione trascendente*.

Lemma 2.1. Sia $\gamma \in \Omega$ e $A \subseteq \Omega$. Allora sono equivalenti:

(a) γ è algebrico su $K(A)$;

(b) $\exists\, \beta_1, \ldots, \beta_n \in K(A)$ tali che $\gamma^n + \beta_1\gamma^{n-1} + \cdots + \beta_n = 0$;

(c) $\exists\, \beta_0, \beta_1, \ldots, \beta_n \in K[A]$, non tutti nulli, tali che $\beta_0\gamma^n + \beta_1\gamma^{n-1} + \cdots + \beta_n = 0$;

(d) $\exists f(x_1, \ldots, x_m, y) \in K[x_1, \ldots, x_m, y]$ e $\alpha_1, \ldots, \alpha_m \in A$ tali che $f(\alpha_1, \ldots, \alpha_m, y) \neq 0$ ma $f(\alpha_1, \ldots, \alpha_m, \gamma) = 0$

Dimostrazione. (a) $\implies$ (b) $\implies$ (c) $\implies$ (a) è ovvio.
(d) $\implies$ (c): scriviamo $f(x_1, \ldots, x_m, y)$ come un polinomio in y a coefficienti nell'anello $K[x_1, \ldots, x_m]$,

$$f(x_1, \ldots, x_m, y) = \sum f_i(x_1, \ldots, x_m) y^{n-i}.$$

quindi vale (c) con $\beta_i = f_i(\alpha_1, \ldots, \alpha_m)$.
(c) $\implies$ (d): i β_i in (c) possono essere espressi come un polinomio in un numero finito di elementi $\alpha_1, \ldots, \alpha_m$ di A, $\beta_i = f_i(\alpha_1, \ldots, \alpha_m)$ con $f_i \in K[x_1, \ldots, x_m]$. Quinid vale (d) con $f = \sum f_i(x_1, \ldots, x_m) y^{n-i}$. □

Definizione 2.2. Se $\gamma \in \Omega$ soddisfa le condizioni del lemma precedente allora si dice che esso è *algebricamente dipendente* su $K(A)$. Un insieme B è detto *algebricamente dipendente* su $K(A)$ se ogni elemento di B è algebricamente dipendente su $K(A)$.

Lemma 2.2. Sia Ω/K un'estensione e sia A un sottoinsieme di Ω che sia algebricamente indipendente su K. Se $\alpha \in \Omega \setminus A$ allora l'insieme $A \cup \{\alpha\}$ è algebricamente indipendente su K se e solo se α è trascendente sul sottocampo $L = K(A)$.

Dimostrazione. ($\implies$) Sia α algebrico su L, dunque $\exists\, f(x) \in L[x], f \neq 0$ tale che $f(\alpha) = 0$. Ogni coefficiente di f ha la forma p/q, dove $p, q \in K[A]$. Semplificando i denominatori, possiamo assumere che tutti i coefficienti di f siano polinomi in A, e dunque esistono elementi $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ e polinomi $p_i \in K[x_1, x_2, \ldots, x_n]$ tali che

$$f(x) = p_r(\alpha_1, \ldots, \alpha_n)x^r + \cdots + p_0(\alpha_1, \ldots, \alpha_n),$$

dove $p_r \neq 0$. Definiamo $g \in K[x_1, x_2, \ldots, x_n, x]$

$$g(x_1, \ldots, x_n, x) = p_r(x_1, \ldots, x_n)x^r + \cdots + p_0(x_1, \ldots, x_n).$$

$g \neq 0$ dato che $p_r \neq 0$ e vale

$$g(\alpha_1, \ldots, \alpha_n, \alpha) = f(\alpha) = 0.$$

Segue che l'insieme $\{\alpha_1, \ldots, \alpha_n, \alpha\}$ non è algebricamente indipendente su K e quindi $A \cup \{\alpha\}$ è algebricamente dipendente.
($\impliedby$) Sia $A \cup \{\alpha\}$ algebricamente dipendente, allora esiste un polinomio non nullo

$$f(x_1, \ldots, x_n, x) \in K[x_1, \ldots, x_n, x]$$

tale che $f(\alpha_1, \ldots, \alpha_n, \alpha) = 0$ con $\alpha_1, \ldots, \alpha_n \in A$ distinti tra loro. Poiché A è algebricamente indipendente, possiamo scrivere

$$f = g_0x^m + g_1x^{m-1} + \cdots + g_m, \qquad g_i \in K[x_1, \ldots, x_n],\ g_0 \neq 0,\ m > 0.$$

Dato che $g_0 \neq 0$ e gli α_i sono algebricamente indipendenti, $g_0(\alpha_1, \ldots, \alpha_n) \neq 0$. Visto che α è radice di

$$f = g_0(\alpha_1, \ldots, \alpha_n)x^m + g_1(\alpha_1, \ldots, \alpha_n)x^{m-1} + \cdots + g_m(\alpha_1, \ldots, \alpha_n)$$

allora è algebrico su $K(\alpha_1, \ldots, \alpha_n) \subset K(A)$.

□

Definizione 2.3. Ω/K è detta *estensione puramente trascendente* se Ω è generato da un insieme A che è algebricamente indipendente su K.

Lemma 2.3. Sia Ω/K un'estensione arbitraria di campi. Allora esiste un campo intermedio $K \leq L \leq \Omega$ tale che L è puramente trascendente su K e Ω è algebrico su L. In particolare, se $A \subseteq \Omega$ genera Ω su K e $A_0 \subseteq A$ è un sottoinsieme massimale per la proprietà che è algebricamente indipendente su K, allora il campo $L = K(A_0)$ ha le proprietà richieste.

Dimostrazione. Osserviamo che se Ω/K è algebrica, allora l'insieme degli elementi di Ω algebricamente indipendenti su K è l'insieme vuoto e così K/K è puramente trascendente. Supponiamo ora che Ω sia generato da A. Dato che per determinare l'indipendenza algebrica è sufficiente considerare un numero finito di elementi alla volta, è facile vedere che il lemma di Zorn si applica a tutti i sottoinsiemi algebricamente indipendenti di A (i quali sono dotati di ordine parziale). Dunque esiste un sottoinsieme $A_0 \subseteq A$ come nell'enunciato del lemma, e sia $L = K(A_0)$. Dato che A_0 è algebricamente indipendente su K, sappiamo che L è puramente trascendente su K, ed ora basta mostrare che Ω è algebrico su L. Gli elementi di $A \setminus A_0$ generano Ω su L, quindi è sufficiente mostrare che questi elementi sono algebrici su L. Sia $\alpha \in A \setminus A_0$, osserviamo dalla massimalità di A_0 che l'insieme $A_0 \cup \{\alpha\}$ non è algebricamente indipendente. Dal Lemma 2.2 ne segue che α è algebrico su $K(A_0) = L$, come richiesto. □

2.2 Basi di Trascendenza

Introduciamo ora per un'estensione Ω/K un concetto che corrisponde per molti versi a quello di 'base' per uno spazio vettoriale.

Definizione 2.4 (Base di trascendenza)**.** Sia Ω/K una arbitraria estensione di campi. Un insieme $A \subseteq \Omega$ che è algebricamente indipendente su K è detto *base di trascendenza* per Ω se Ω è algebrico su $K(A)$.

Osservazione: Dal Lemma 2.3 si deduce che ogni estensione di campi ha una base di trascendenza, ed ogni estensione finitamente generata ha una base di trascendenza finita (di cardinalità che non eccede quella dell'insieme generatore). Notiamo inoltre che una estensione è algebrica se e solo se la base di trascendenza è l'insieme vuoto.

Ora ci occuperemo di dimostrare che la cardinalità di una base di trascendenza è univocamente determinata. Dunque potremo considerare in teoria dei campi un concetto di dimensione in modo analogo a quanto avviene per gli spazi vettoriali.

Lemma 2.4. Sia Ω/K un'estensione e supponiamo $A, B \subseteq \Omega$ disgiunti con A algebricamente indipendente su K. Sia $L = K(A)$. $A \cup B$ è algebricamente indipendente su K se e solo se B è algebricamente indipendente su L.

Dimostrazione. ($\Longrightarrow$) Sia $A \cup B$ algebricamente indipendente. Assumiamo che B sia finito e dimostriamo per induzione su $n = |B|$ che B è indipendente su L. Se $n = 0$ la tesi è dimostrata dal fatto che l'insieme vuoto è sempre algebricamente indipendente su un campo. Assumiamo allora $n > 0$ e prendiamo $\beta \in B$. sia $B' = B \setminus \{\beta\}$. Per ipotesi induttiva sappiamo che B' è algebricamente indipendente su L, e quindi per il Lemma 2.2 è sufficente mostrare che β è trascendente su $L(B')$. Ora $A \cup B$ è algebricamente indipendente su K, e dunque dal Lemma 2.2 sappiamo che β è trascendente su $K(A \cup B')$. La dimostrazione si conclude notando che $K(A \cup B') = L(B')$.
($\Longleftarrow$) Supponiamo ora che B sia algebricamente indipendente su L. Per mostrare che $A \cup B$ è algebricamente indipendente su K, non è restrittivo assumere che B sia finito. Dimostriamo l'asserto ancora per induzione su $n = |B|$. Se $n = 0$ non c'è nulla da provare poiché, per ipotesi, A è algebricamente indipendente su K. Assumiamo quindi $n > 0$ e prendiamo $\beta \in B$. Sia $B' = B \setminus \{\beta\}$. Per ipotesi induttiva, $A \cup B'$ è indipendente su K, e dunque per il Lemma 2.2 è sufficiente mostrare che β è trascendente su $K(A \cup B') = L(B')$. Ma ciò è vero per il Lemma 2.2 dal fatto che $B = B' \cup \{\beta\}$ è indipendente su L. □

Teorema 2.1. Sia Ω/K un'estensione e sia Ω algebrico su $K(A)$ per qualche sottoinsieme finito $A \subseteq \Omega$. Allora ogni sottoinsieme $B \subseteq \Omega$ tale che $|B| > |A|$ è algebricamente dipendente su K.

Dimostrazione. Dato che $|B| > 0 \; \exists \beta \in B \neq \emptyset$. Se β è algebrico su K, allora B è dipendente dunque possiamo assumere β trascendente su K. Quindi Ω non è algebrico su K e $|A| > 0$. Si presentano due casi: $\beta \in A$ oppure $\beta \notin A$

- $\beta \in A$: (Per induzione su $|A|$) definiamo $A' = A \setminus \{\beta\}$ e $B' = B \setminus \{\beta\}$ e $L = K(\beta)$. Ora Ω è algebrico su $K(A) = L(A')$ e poiché $|B'| > |A'|$, l'ipotesi induttiva implica che B' è algebricamente dipendente su L. Dato che $B = B' \cup \{\beta\}$ è un'unione disgiunta, B' è algebricamente dipendente su L e $L = K(\beta)$, per il lemma precedente B è algebricamente indipendente su K.

- $\beta \notin A$: mostriamo come rimpiazzare A con un nuovo insieme $C \subseteq \Omega$ tale che $|C| \leq |A|$, Ω algebrico su $K(C)$ e $\beta \in C$ (ciò terminerebbe la dimostrazione dato che rientreremmo nel caso appena dimostrato). Dato che β è trascendente su K, l'insieme $\{\beta\}$ è algebricamente indipendente su K e possiamo imporre $C \supseteq \{\beta\}$ sia sottoinsieme di $A \cup \{\beta\}$, massimale per la proprietà che è indipendente su K. Dato che β è algebrico su $K(A)$, il Lemma 2.2 garantisce che $A \cup \{\beta\}$ non è indipendente su K. Segue che C è sottoinsieme proprio di $A \cup \{\beta\}$ dunque $|C| \leq |A|$ come richiesto. Per vedere che Ω è algebrico su $K(C)$, osserviamo che il Lemma 2.3 ci dice che $K(A \cup \{\beta\})$ è algebrico su $K(C)$. Dato che Ω è algebrico su $K(A)$, è certamente algebrico su $K(A \cup \{\beta\})$ e segue che Ω è algebrico su $K(C)$. Infine $\beta \in C$ per costruzione.

□

Corollario 2.1. Sia A una base di trascendenza finita di Ω su K. Allora tutte le basi di trascendenza di Ω/K hanno la stessa cardinalità.

Dimostrazione. Per ipotesi $|A| < \infty$. dato che Ω è algebrico su $K(A)$, il Teorema 2.1 ci assicura che nessun insieme algebricamente indipendente può avere cardinalità maggiore di quella di A (e in particolare nessuno può essere infinito). Sia B un'altra base di trascendenza, abbiamo $|B| \leq |A|$. Interscambiando il ruolo delle due basi, otteniamo la disegualianza inversa, dunque è verificata la tesi. □

Osservazione 1: Sia A una base di trascendenza per Ω/K avente $n < \infty$ elementi. Allora per il corollario precedente ogni base di trascendenza ha cardinalità n. In questo caso diciamo che il *grado* di *trascendenza* dell'estensione è n, e scriviamo $td_K(\Omega) = n$.

Osservazione 2: È possibile estendere il corollario precedente per mostrare che anche se sono infinite entrambe le basi di trascendenza di Ω/K, esse devono avere la stessa cardinalità. Notiamo inoltre che $td_K(\Omega) = 0$ se e solo se Ω è algebrico su K.

Osservazione 3: $td_K(\Omega)$ è finito se e solo se Ω è algebrico su qualche campo intermedio $K \leq L \leq \Omega$, dove L è finitamente generato su K. Se $td_K(\Omega) < \infty$ è immediato dalla definizione che L esiste; viceversa, se abbiamo L finitamente generato su K, allora L ha una base di trascendenza finita su K. Se Ω è algebrico su L, questa base è anche una base di trascendenza per Ω su K.

Esempi: $\mathbb{R}/\mathbb{Q}$ e $\mathbb{C}/\mathbb{Q}$ sono estensioni trascendenti con grado di trascendenza infinito; $K(x_1, \ldots, x_n)/K$, con $\{x_1, \ldots, x_n\}$ un insieme finito di indeterminate algebricamente indipendenti, è un'estensione puramente trascendente con grado di trascendenza n.

2.3 Teorema di Lüroth

Supponiamo che Ω/K sia un'estensione finitamente generata con grado di trascendenza n. Se $\{\alpha_1, \ldots, \alpha_n\}$ è una base di trascendenza per Ω/K allora $\Omega/K(\alpha_1, \ldots, \alpha_n)$ è un'estensione finita. Se è possibile trovare una base di trascendenza $\{\alpha_1, \ldots, \alpha_n\}$ per Ω/K tale che $\Omega = K(\alpha_1, \ldots, \alpha_n)$ allora Ω è puramente trascendente su K. In generale non è semplice determinare se un'estensione finitamente generata è puramente trascendente oppure no. C'è comunque un caso dove il problema si risolve senza troppe difficoltà, come vedremo nel teorema di Lüroth. Prima di procedere ricordiamo un noto lemma importante ai fini della dimostrazione:

Lemma 2.5 (Lemma di Gauss)**.** Sia D un dominio a fattorizzazione unica ed F il suo campo delle frazioni. Siano $f, g \in D[x]$: se f divide g in $F[x]$ e f è primitivo, allora f divide g in $D[x]$.

Definiamo il grado $deg(u)$ di un elemento $u \in K(t)$ come il maggiore tra i gradi del numeratore e del denominatore di u, espresso nella sua forma semplice. Allora vale il seguente

Lemma 2.6. Sia $u \in K(t) \setminus K$. Allora u è trascendente su K, t è algebrico su $K(u)$, e $[K(t) : K(u)] = deg(u)$.

Teorema 2.2 (Teorema di Lüroth)**.** Sia $\Omega = K(t)$ con t trascendente su K. Allora ogni sottocampo L di Ω che contiene propriamente K è della forma $L = K(u)$ per qualche $u \in \Omega$ trascendente su K.

Dimostrazione. Sia $u \in L \setminus K$,

$$[K(t) : L] \leq [K(t) : K(u)] = deg(u)$$

e quindi t è algebrico su L. Sia

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in L[x],\ n = [K(t) : L]$$

il suo polinomio minimo. Dato che t è trascendente su K, qualche $a_j \notin K$. Mostreremo che $L = K(a_j)$ per qualche a_j. Sia $d(t) \in K[t]$ un polinomio di grado minimo tale che $d(t)a_i(t) \in K[t]$ per ogni i, e sia

$$f_1(t, x) = df(x) = dx^n + da_1 x^{n-1} + \cdots + da_n \in K[t, x].$$

Allora f_1 è primitivo come polinomio in x, così $MCD(d, da_1, \ldots, da_n) = 1$ in $K[t]$. Il grado m di f_1 in t è il grado maggiore di uno dei polinomi $da_1, da_2, \ldots$, diciamo $m = deg(da_i)$. scriviamo $a_i = \frac{b}{c}$ con b, c polinomi coprimi in $K(t)$. Ora $b(x) - c(x)a_i(t)$ è un polinomio in $L[x]$ che ha t come radice, e quindi è divisibile per f:

$$f(x) \cdot q(x) = b(x) - c(x) \cdot a_i(t),\ q(x) \in L[x].$$

Moltiplicando ambo i membri per $c(t)$, troviamo

$$c(t) \cdot f(x) \cdot q(x) = c(t) \cdot b(x) - c(x) \cdot b(t).$$

Dato che f_1 differisce da f per un elemento non nullo in $K(t)$, l'equazione mostra che f_1 divide $c(t) \cdot b(x) - c(x) \cdot b(t)$ in $K(t)[x]$, ma f_1 è primitivo in $K[t][x]$ e quindi divide il polinomio in $K[t][x] = K[t, x]$ per il Lemma 2.5, perciò esiste un polinomio $h \in K[t, x]$ tale che

$$f_1(t, x) \cdot h(t, x) = c(t) \cdot b(x) - c(x) \cdot b(t). \tag{2.1}$$

Nella (2.1) il polinomio $c(t) \cdot b(x) - c(x) \cdot b(t)$ ha grado al massimo m in t, ed m è il grado di $f_1(t, x)$ in t. Quindi $c(t) \cdot b(x) - c(x) \cdot b(t)$ ha grado esattamente m in t e $h(t, x)$ ha grado 0 in t, dunque $h \in K[x]$. Dalla (2.1) segue che $c(t) \cdot b(x) - c(x) \cdot b(t)$ non è divisibile per un polinomio non costante in $K[t]$. Il polinomio $c(t) \cdot b(x) - c(x) \cdot b(t)$ è simmetrico in t e in x, quindi non cambia quando vengono interscambiate. Perciò ha grado m in x e non è divisibile per un polinomio non costante in $K[x]$. Segue da (2.1) che h non è divisibile per un polinomio non costante in $K[x]$ e quindi $h \in K^*$. Concludiamo che $f_1(t, x)$ è un multiplo di $c(t) \cdot b(x) - c(x) \cdot b(t)$. Comparando i gradi in x in (2.1), vediamo che $n = m$. Così

$$[K(t) : K(a_i)] \overset{2.6}{=} deg(a_i) \leq deg(da_i) = m = n = [K(t) : L] \leq [K(t) : K(a_i)].$$

Quindi vale l'uguaglianza e dunque $L = K[a_i]$. Infine, se $a_j \notin K$, allora

$$[K(t) : L] \leq [K(t) : K(a_j)] \overset{2.6}{=} deg(a_j) \leq deg(da_j) \leq deg(da_i) = m = [K(t) : L],$$

e perciò $L = K(a_j)$. □

Capitolo 3

Estensioni di Galois infinite

Tratteremo ora il problema di estendere il teorema fondamentale della teoria di Galois finita alle estensioni di Galois infinite. Ciò sarà utile per poter, nell'ultimo capitolo di questo elaborato, affrontare la teoria di Galois trascendente. Nel passaggio dalle estensioni finite a quelle infinite non è più vero che tutti i sottogruppi del gruppo di Galois fissano una certa estensione intemedia L/K: il primo esempio di un sottogruppo di questo tipo fu trovato da Dedekind agli inizi del ventesimo secolo. Fu invece il matematico tedesco Wolfgang Krull che trovò una soluzione al problema dotando il gruppo di Galois di una topologia che fu poi chiamata *Topologia di Krull*. Andiamo ad approfondire ora le nozioni di gruppo topologico e la topologia appena citata.

3.1 Gruppi topologici

Definizione 3.1. Un insieme G dotato di una struttura di gruppo e di una topologia è detto *gruppo topologico* se le mappe

$$G \times G \to G : (g, h) \mapsto gh$$

$$G \to G : g \mapsto g^{-1}$$

sono entrambe continue.

Se a è un elemento di un gruppo topologico G allora $a_S : G \to G$, $g \mapsto ag$ è continua perchè composizione di

$$G \overset{g\mapsto(a,g)}{\longrightarrow} G \times G \overset{(g,h)\mapsto gh}{\longrightarrow} G.$$

Di fatto è un omeomorfismo con inversa $(a^{-1})_S$. In maniera analoga $a_D : g \mapsto ga$ e $g \mapsto g^{-1}$ sono entrambi omeomorfismi. Dunque per un sottogruppo H di G, la classe laterale sinistra aH di H è aperta o chiusa a seconda che H sia aperto o chiuso. Inoltre vale:

Lemma 3.1. Sia G un gruppo topologico e H un sottogruppo di G. allora:

a) se H è aperto allora è chiuso;

b) se H è chiuso e di indice finito allora è aperto. In particolare, se G è compatto e H è chiuso, H è aperto se e solo se è di indice finito.

Dimostrazione. Sia H un sottogruppo aperto di G. Allora $G = \bigcup_{a\in G} aH$ e di conseguenza abbiamo che $H = G\backslash\bigcup_{a\in G, a\neq 1_G} aH$. Dato che aH è aperto tale unione arbitraria è ancora un aperto di G, il che significa che H è il complementare di un insieme aperto quindi è chiuso. Sia ora H un sottoinsieme chiuso di indice finito di G. Dunque esiste un numero finito di elementi $a_1, \ldots, a_n \in G$ tali che $G = \bigcup_{i=1}^{n} a_i H$. Dato che gli $a_i H$ sono chiusi per ipotesi, la loro unione finita è ancora chiusa e quindi H è il complementare di un insieme chiuso dunque è aperto. Sia ora G compatto e H un sottoinsieme chiuso. Se H ha indice finito allora è aperto per ciò che abbiamo appena provato. Viceversa, se H è aperto allora la famiglia di insiemi aperti $\{aH : a \in G\}$ è un ricoprimento per G. Essendo G compatto, esistono $a_1, \ldots, a_n \in G$ tali che $G = \bigcup_{i=1}^{n} a_i H$. Ciò implica che H è di indice finito. □

Definizione 3.2. Una *Base di Intorni* per un punto x di uno spazio topologico X è una famiglia N di intorni di x tale che per ogni sottoinsieme aperto M di X contenente x esista un N $\in N$ tale che N $\subset M$.

Proposizione 3.1. Sia G un gruppo topologico, e sia N una base di intorni per l'identità e di G. allora valgono le seguenti:

(a) $\forall$ N_1, $N_2 \in N$, esiste un N' $\in N$ tale che $e \in$ N' $\subset N_1 \cap N_2$;

(b) $\forall$ N $\in N$, esiste un N' $\in N$ tale che N'N' $\subset$ N;

(c) $\forall$ N $\in N$, esiste un N' $\in N$ tale che N' $\subset N^{-1}$;

(d) $\forall$ N $\in N$ e $\forall g \in G$, esiste un N' $\in N$ tale che N' $\subset gNg^{-1}$;

(e) $\forall g \in G$, $\{gN : N \in N\}$ è una base di intorni per g.

Viceversa, se G è un gruppo e N è un insieme non vuoto di sottoinsiemi di G che soddisfa (a,b,c,d), allora c'è un unica topologia su G per la quale vale (e).

3.2 La Topologia di Krull

Ricordiamo che un'estensione Ω/K è di Galois se è finita, normale e separabile il che equivale a dire che ogni polinomio irriducibile $f \in K[x]$ che ha una radice in Ω, ha $deg(f)$ radici disitinte in Ω. Nel caso infinito definiamo le estensioni di Galois allo stesso modo omettendo l'ipotesi di finitezza. Se Ω/K è un'estensione di Galois, il gruppo di Galois, che denotiamo con $Gal(\Omega/K)$, è il gruppo degli automorfismi di Ω che tiene fisso K.

Proposizione 3.2. Sia Ω/K un'estensione di Galois. Se L è un campo intermedio $K \leq L \leq \Omega$ allora Ω/L è di Galois.

Dimostrazione. Per le proprietà note nel caso finito sappiamo che: se Ω/K è separabile, allora Ω/L e L/K sono separabili; se Ω/K è normale, allora Ω/L è normale. Dunque l'estensione Ω/L è normale e separabile, quindi di Galois. □

Ricordiamo che, nelle ipotesi della proposizione precedente, non è sempre vero che l'estensione L/K è di Galois dal fatto che non è garantita la condizione di normalità dell'estensione.

Proposizione 3.3. Sia Ω/K di Galois e sia L un campo intermedio $K \leq L \leq \Omega$. Allora ogni K-omomorfismo $L \to \Omega$ si estende ad un K-omomorfismo $\Omega \to \Omega$.

Dimostrazione. La dimostrazione che un K-omomorfismo tra L e Ω si estende ad un omomorfismo $\alpha : \Omega \to \Omega$ si può trovare in [3, p. 90]. Consideriamo $a \in \Omega$ e il suo polinomio minimo f su K. Ω contiene esattamente $deg(f)$ radici di f, e quindi anche $\alpha(\Omega) \subset \Omega$. Dunque $a \in \alpha(\Omega)$ e ciò mostra che α è suriettivo. □

Definizione 3.3. Sia Ω/K un'estensione di Galois. Un sottoinsieme $S \subset \Omega$ è *G-stabile* se preso $\sigma \in G$ risulta $\sigma(S) \subset S$.

Sia Ω/K un'estensione di Galois, e sia $G = Gal(\Omega/K)$. Per un sottoinsieme finito S di Ω consideriamo

$$G_S = \{\sigma \in G : \sigma(s) = s \ \forall s \in S\}.$$

Notiamo che $G_S = Aut(\Omega/K(S))$, dove $K(S)$ è l'estensione di K generata da S. Con la famiglia di insiemi $\{G_S\}_{S \subset \Omega \, finito}$ vogliamo indurre una topologia sul gruppo $Gal(\Omega/K)$.

Proposizione 3.4. Sia Ω/K di Galois. Per ogni campo intemedio L che sia finito e di Galois su Ω, la mappa

$$\phi_L : Gal(\Omega/K) \to Gal(L/K), \ \sigma \mapsto \sigma|_L$$

è continua e suriettiva.

Dimostrazione. Consideriamo $\sigma \in Gal(L/K)$ un K-omomorfismo tra L e Ω. σ può essere esteso ad un K-automorfismo in Ω grazie alla Proposizione 3.3, che mostra la suriettività di ϕ_L. Per ogni insieme finito S di generatori di L su K, $Gal(\Omega/L) = G_S$, il che mostra che l'anti-immagine di $1_{Gal(L/K)}$ è aperta in G. Ciò vale per ogni elemento di $Gal(L/K)$. □

Lemma 3.2. Sia Ω/K un'estensione di Galois e sia $S \subset \Omega$ un insieme finito G-stabile. Allora abbiamo una successione esatta di gruppi

$$1 \to G_S \to Gal(\Omega/K) \xrightarrow{\pi} Gal(K(S)/K) \to 1.$$

Dunque G_S è un sottogruppo aperto e normale di G di indice finito.

Dimostrazione. Notiamo inanzitutto che per un tale S, $K(S)/K$ è di Galois. Sappiamo che è separabile dunque basta dimostrare che è normale. Per $\alpha \in S$, sia f_α il polinomio minimo irriducibile di α su K. Poiché S è G-stabile, ogni radice di f_α è in S. Quindi $K(S)$ è il campo di spezzamento di f_α dunque è un'estensione normale. Dimostriamo ora che $Ker(\pi) = G_S$: se $\sigma \in Ker(\pi)$ allora $\sigma|_{K(S)} = id$, quindi $\sigma|_S = id$ e $\sigma \in G_S$; viceversa se $\sigma \in G_S$ allora $\sigma|_K = id$ e $\sigma|_S = id$ e poiché $K(S)$ è generata da S su K, $\sigma|_{K(S)} = id$ quindi $\sigma \in Ker(\pi)$. Dunque $Ker(\pi) = G_S$. Per la Proposizione 3.4, π è continua e suriettiva dunque la successione è esatta. Poiché π è continua, il Kernel G_S è un sottogruppo aperto e normale. □

Proposizione 3.5. Esiste un'unica struttura di gruppo topologico su G per la quale gli insiemi G_S formano una base di intorni aperti di 1. Per questa topologia gli insiemi G_S, con S G-stabile, sono aperti e normali.

Dimostrazione. Dimostriamo che la collezione di insiemi G_S soddisfa (a,b,c,d) della Proposizione 3.1: soddisfa (a) poiché $G_{S_1} \cap G_{S_2} = G_{S_1 \cup S_2}$; soddisfa inoltre (b) e (c) poiché ogni inisieme G_S è un gruppo. Sia ora S un sottoinsieme finito di Ω. Allora $K(S)$ è un'estensione finita di K e quindi c'è solo un numero finito di K-omomorfismi $K(S) \to \Omega$. Poiché $\sigma(S) = \tau(S)$ se $\sigma|_{K(S)} = \tau|_{K(S)}$, $\bar{S} = \bigcup_{\sigma \in G} \sigma(S)$ è finito. Ora $\sigma(\bar{S}) = \bar{S}$ $\forall \sigma \in G$, perciò segue che $G_{\bar{S}}$ è normale in G. Da cui $\sigma(G_{\bar{S}})\sigma^{-1} = G_{\bar{S}} \subset G_S$, che prova (d). La seconda affermazione è dimostrata nel lemma precedente. □

La topologia sul gruppo $Aut(\Omega/K)$ definita nella proposizione precedente è detta *Topologia di Krull*. Scriveremo $Gal(\Omega/K)$ per $Aut(\Omega/K)$ dotata della topologia di Krull e chiameremo questo gruppo Gruppo di Galois di Ω/K.

Se S è un insieme finito G-stabile allora $K(S)$ è un'estensione finita G-stabile di K e dunque di Galois su K. Pertanto $\{Gal(\Omega/L) : L \text{ è finito e di Galois su } K\}$ è una base di intorni di 1 composta da sottogruppi aperti e normali.

Proposizione 3.6. Il gruppo di Galois G di un'estensione Ω/K è di Hausdorff, compatto e totalmente disconnesso.

Dimostrazione. Dimostriamo che G è di Hausdorff. Se $\sigma \neq \tau$ allora $\sigma^{-1}\tau \neq 1$ e quindi esiste un $a \in \Omega$ tale che $\sigma(a) \neq \tau(a)$. Per un sottoinsieme S contenente a, $\sigma(G_S)$ e $\tau(G_S)$ sono disgiunti poiché i loro elementi agiscono differentemente su a. Quindi sono sottoinsiemi aperti e disgiunti di G contenenti rispettivamente σ e τ. Le due proprietà mancanti del gruppo di Galois sono dimostrate nel [3, p. 96].

□

Proposizione 3.7. Per ogni estensione di Galois Ω/K risulta $\Omega_{Gal(\Omega/K)} = K$

Dimostrazione. Ogni elemento di Ω/K appartiene ad un'estensione di Galois finita su K. La tesi segue dalla suriettività dimostrata nella Proposizione 3.4. □

3.3 Teorema fondamentale della teoria di Galois infinita

Proposizione 3.8. Sia Ω/K un'estensione di Galois con $G = Gal(\Omega/K)$.

a) Sia L un campo intermedio $K \leq L \leq \Omega$. Allora Ω è di Galois su L, $Gal(\Omega/L)$ è chiuso in G e $\Omega_{Gal(\Omega/L)} = L$.

b) Per ogni sottogruppo H di G, $Gal(\Omega/\Omega_H)$ è la chiusura di H in G.

Dimostrazione. **a)** la prima affermazione è dimostrata nella 3.2. Per ogni insieme finito $S \subset L$, G_S è un sottogruppo aperto di G e quindi è chiuso. Dato che $Gal(\Omega/L) = \bigcap_{S \subset L} G_S$ allora è chiuso. L'ultima affermazione è dimostrata nella 3.7.

b) Poiché $Gal(\Omega/\Omega_H)$ è un insieme chiuso contenente H, contiene certamente la chiusura $\bar{H}$ di H. Consideriamo ora $\sigma \in G \setminus \bar{H}$ e mostriamo che σ non fissa alcuni elementi di Ω_H. Dato che $\sigma \notin \bar{H}$,

$$\sigma(Gal(\Omega/L)) \cap H = \emptyset$$

per qualche estensione di Galois finita L/K in Ω (poiché l'insieme $Gal(\Omega/L)$ forma una base di intorni per 1). Denotiamo con ϕ la mappa suriettiva $Gal(\Omega/K) \to Gal(L/K)$. Allora $\sigma|_L \notin \phi(H)$ e quindi σ muove alcuni elementi di $L_{\phi(H)} \subset \Omega_H$.

□

Teorema 3.1 (Teorema Fondamentale della Teoria di Galois)**.** Sia Ω/K un'estensione di Galois con gruppo di Galois G. allora le mappe:

$$H \mapsto \Omega_H,\ L \mapsto Gal(\Omega/L)$$

sono anti-isomorfismi, l'uno inverso dell'altro, tra il reticolo dei sottogruppi chiusi di G e il reticolo dei campi intemedi tra Ω e K. Inoltre:

a) $H_1 \supset H_2 \iff \Omega_{H_1} \subset \Omega_{H_2}$;

b) un sottogruppo chiuso H di G è aperto se e solo se Ω/H ha grado finito su K, in questo caso $(G : H) = [\Omega_H : K]$;

c) $\sigma H \sigma^{-1} \leftrightarrow \sigma L$, cioè

$$\Omega_{\sigma H \sigma^{-1}} = \sigma(\Omega_H);$$
$$Gal(\Omega/\sigma(L)) = \sigma Gal(\Omega/L)\sigma^{-1};$$

d) un sottogruppo chiuso H di G è normale se e solo se Ω_H è di Galois su K e in questo caso

$$Gal(\Omega_H/K) \simeq G/H.$$

Sono sottolineate le parole chiave che evidenziano le differenze tra il teorema fondamentale di Galois nel caso infinito e quello finito.

Capitolo 4

Teoria di Galois Trascendente

Come abbiamo potuto osservare nello scorso capitolo, Krull generalizza la teoria di Galois dimostrando che se Ω è un'estensione normale e separabile di K allora il gruppo di Galois associato può essere dotato di una topologia per la quale esiste un anti-isomorfismo reticolare tra i campi intermedi di Ω/K e i sottogruppi topologicamente chiusi di G. Nella Proposizione 3.6 abbiamo visto che G diventa così un gruppo topologico compatto e di Hausdorff. Quando Ω/K è finita la teoria di Krull si riconduce alla corrispondenza di Galois classica.

Viene spontaneo chiedersi se si possa considerare per un'estensione Ω/K non necessariamente algebrica una opportuna topologia sul gruppo di Galois G che consenta di ristabilire una corrispondenza analoga a quella di Krull-Galois nel caso più generale.

4.1 La corrispondenza di Galois trascendente

Definizione 4.1. sia Ω/K un'estensione arbitraria di campi. Diciamo che Ω/K è un'estensione di Galois se K coincide con il campo fissato da tutti gli automorfismi di Ω su K. Il gruppo degli automorfismi di Ω/K è detto gruppo di Galois di Ω/K e lo indichiamo con $Gal(\Omega/K)$.

Teorema 4.1. Siano Ω un campo algebricamente chiuso e K un sottocampo perfetto di Ω. Se $\alpha \in \Omega$ è fissato da ogni K-automorfismo di Ω, allora $\alpha \in K$, così $\Omega_{Aut(\Omega/K)} = K$.

Dimostrazione. Sia $\alpha \in \Omega \setminus K$. Se α è algebrico su K, allora esiste un K-omomorfismo $K[\alpha] \to \Omega$ che manda α in un coniugato di α in Ω diverso da α. Questo omomorfismo si estende ad un isomorfismo $K^{alg} \to K^{alg} \subset \Omega$, dove K^{alg} è la chiusura algebrica di K in Ω (per il [3, pag. 90 Theorem 6.6]). Ora prendiamo una base trascendente A per Ω su K^{alg}. Possiamo estendere l'isomorfismo ad un isomorfismo $K^{alg}(A) \to K^{alg}(A) \subset \Omega$ mandando ogni elemento di A in se stesso. Infine possiamo estendere questo isomorfismo ad un isomorfismo dalla chiusura algebrica Ω di $K^{alg}(A)$ a Ω. Se α è trascendente su K allora appartiene ad una base trascendente A per Ω su K. Se $A \neq \{\alpha\}$ allora esiste un automorfismo σ di A tale che $\sigma(\alpha) \neq \alpha$. Ora σ definisce un K-omomorfismo $K(A) \to \Omega$, il quale si estende ad un isomorfismo $\Omega \to \Omega$ come prima. Se $A = \{\alpha\}$ allora possiamo

porre $K(\alpha) \to \Omega$ il K-omomorfismo che manda $\alpha \mapsto \alpha + 1$. Allo stesso modo, esso si estende ad un isomorfismo $\Omega \to \Omega$. □

Definizione 4.2. Sia Ω/K un'estensione di Galois e sia G il gruppo di Galois di Ω su K. Sia $\alpha \in \Omega$ e definiamo $G(\alpha) = \{\sigma \in G : \sigma(\alpha) \neq \alpha\}$. Se τ e ρ sono elementi di G, denotiamo $\tau G(\alpha)\rho = \{\tau\sigma\rho : \sigma \in G(\alpha)\}$. Sia F la collezione di tutti gli insiemi $\tau G(\alpha)\rho$, con τ e ρ in G e α in Ω. Se $G(\alpha) = \emptyset$ poniamo $\tau G(\alpha)\rho = \emptyset$.

La collezione F costituisce una sottobase di insiemi aperti per una topologia $\mathcal{T}$ su G, cioè una base per $\mathcal{T}$ è formata dagli insiemi della forma

$$\tau_1 G(\alpha)\rho_1 \cap \tau_2 G(\alpha)\rho_2 \cap \cdots \cap \tau_n G(\alpha)\rho_n.$$

È possibile dimostare che, dotato della topologia così definita, il gruppo $(G, \mathcal{T})$ è un gruppo topologico. Inoltre esso ha una sottobase di insiemi aperti formata da insiemi della forma $\sigma G(\beta)$, $\sigma \in G$, $\beta \in \Omega$.

La topologia appena introdotta, che per semplicità denoteremo con $\mathcal{T}$, è detta *topologia di Soundararajan e Venkatachaliengar*. Vedremo nel Teorema 4.4 che tale topologia coincide con la topologia di Krull se e solo se l'estensione Ω/K è algebrica.

Lemma 4.1. Sia G un gruppo e sia $G_1, G_2, \ldots, G_r, H$ un numero finito di sottogruppi di G. Sia H contenuto nell'unione di un numero finito di classi laterali sinistre dei G_i. Allora H è contenuto nell'unione di un numero finito di classi laterali di $G_1 \cap \cdots \cap G_r$.

Dimostrazione. Vedi [6, Lemma 1.1] □

Definizione 4.3. Sia Ω/K un'estensione di campi. Diciamo che Ω è un'*Estensione di Dedekind* di K se per ogni campo intermedio $K \leq L \leq \Omega$, Ω è di Galois su L.

Teorema 4.2. Sia Ω/K un'estensione di Dedekind. Sia G il gruppo di Galois di Ω su K e sia $\mathcal{T}$ la topologia introdotta nella Definizione 4.2. Allora esiste una corrispondenza biunivoca tra i campi intermedi di Ω/K e tutti i sottogruppi di G che siano chiusi per la topologia $\mathcal{T}$.

Dimostrazione. $G_L = \{\sigma \in G : \sigma(l) = l \ \forall l \in L\} \leq G$ è il gruppo di Galois di Ω su L. Per ipotesi, poiché Ω è di Galois su L, abbiamo che L è il campo fissato dagli elementi di $G_L = Gal(\Omega/L)$, così $\Omega_{Gal(\Omega/L)} = L$. Se H è un sottogruppo chiuso di G che fissa un'estensione intermedia allora abbiamo $G_{\Omega_H} = H$. Segue che esiste una corrispondenza di Galois biuniovoca tra i campi intermedi di Ω/K ed i sottogruppi chiusi di G che fissano un'estensione intermedia. Dunque rimane da mostrare che un sottogruppo H di G fissa una certa estensione intermedia se e solo se H è chiuso per la topologia $\mathcal{T}$. Lo dimostriamo nel seguente teorema: □

Teorema 4.3. Sia Ω/K un'estensione di Galois alla quale è associato il gruppo di Galois G. Allora esiste una topologia $\mathcal{J}$ su G tale che i sottogruppi di G che fissano una certa estensione intermedia di Ω/K sono esattamente i sottogruppi chiusi per la topologia $\mathcal{J}$.

Dimostrazione. Consideriamo la topologia $\mathcal{T}$ introdotta nella definizione 4.2. Sia H un sottogruppo di G che fissa una certa estensione intermedia L di Ω/K. Sia τ un elemento di $G \setminus H$. Allora esiste un elemento $\alpha \in L$ tale che $\tau(\alpha) \neq \alpha$. consideriamo ora $G(\alpha)$ introdotto nella definizione 4.2. $G(\alpha)$ è un insieme $\mathcal{T}$-aperto e $\tau \in G(\alpha)$. Poiché $\alpha \in L = \Omega_H$, nessun elemento di H appartiene a $G(\alpha)$. Dunque per ogni $\tau \in G \setminus H$ esiste un insieme $\mathcal{T}$-aperto che contiene τ che è completamente contenuto in $G \setminus H$. Dunque $G \setminus H$ è aperto e quindi H è $\mathcal{T}$-chiuso.

Viceversa sia ora H un sottogruppo di G che sia chiuso per la topologia $\mathcal{T}$. Mostriamo che H fissa un certo campo intermedio L di Ω/K. Sia σ un elemento di G che fissa ogni elemento di L. Dobbiamo mostrare che $\sigma \in H$. Affermiamo che ogni intorno di σ interseca H. È sufficiente mostrare che ogni insieme aperto di base che contiene σ interseca H. Possiamo prendere come insieme aperto di base contenente σ l'insieme

$$\tau_1 G(\alpha_1) \cap \tau_2 G(\alpha_2) \cap \cdots \cap \tau_n G(\alpha_n).$$

Si presentano ora due casi:

Caso 1: ogni elemento $\alpha_1, \alpha_2, \ldots, \alpha_n$ è algebrico su L. Quindi ogni α_i ha solo un numero finito di immagini distinte $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ir_i}$ per H. Se consideriamo tutte le funzioni simmetriche elementari sugli $\alpha_{i1}, \ldots, \alpha_{ir_i}$, allora essi sono fissati da ogni elemento di H e quindi appartengono a L. Dunque il polinomio $(x - \alpha_{i1}) \cdots (x - \alpha_{ir_i})$ è irriducibile su L. Segue che α_i è un elemento algebrico separabile su L. Dunque il sottocampo $L(\alpha_1, \ldots, \alpha_n)$ e contenuto in un'estensione finita normale e separabile

$$M = L(\alpha_{11}, \ldots, \alpha_{1r_1}, \alpha_{21}, \ldots, \alpha_{2r_2}, \ldots, \alpha_{n1}, \ldots, \alpha_{nr_n})$$

di L e quindi $M \leq \Omega$. Poiché un'estensione finita e separabile è semplice abbiamo $M = L(\beta)$. Ora ogni automorfismo di Ω su L induce un automorfismo di M su L poiché M è finito normale e separabile su L. Come prima, se $\{\beta_1 = \beta, \beta_2, \ldots, \beta_m\}$ è l'insieme completo delle distinte immagini di β per H allora $(x-\beta_1) \cdots (x-\beta_m)$ è un polinomio irriducibile su L ed ogni automorfismo di M su L deve mandare β in qualche β_i. Quindi $\beta \mapsto \beta_i$ $i = 1, 2, \ldots, m$ costituisce l'insieme completo degli automorfismi di M su L. Inoltre, preso $i \in \{1, 2, \ldots, m\}$ esiste un elemento di H che manda β in β_i. Ora σ induce inoltre un automorfismo di M su L poiché σ tiene fisso ogni elemento di L. Ma H induce l'insieme completo di automorfismi di M su L. Capiamo quindi che esiste un elemento $h \in H$ tale che σ e h inducono gli stessi automorfismi di M su L. Poiché $\alpha_i \in M$ abbiamo $\sigma(\alpha_i) = h(\alpha_i)$. Dunque $\tau_i^{-1}(\sigma(\alpha_i)) = \tau_i^{-1}(h(\alpha_i))$. Così $(\tau_i^{-1}\sigma)(\alpha_i) = (\tau_i^{-1}h)(\alpha_i)$. Poiché $\sigma \in \tau_i G(\alpha_i)$ abbiamo $\tau_i^{-1}\sigma \in G(\alpha_i)$ e dunque $(\tau_i^{-1}\sigma)(\alpha_i) \neq \alpha_i$ quindi segue che $h \in \tau_1 G(\alpha_1) \cap \tau_2 G(\alpha_2) \cap \cdots \cap \tau_n G(\alpha_n)$. Quindi questo insieme aperto $\tau_1 G(\alpha_1) \cap \tau_2 G(\alpha_2) \cap \cdots \cap \tau_n G(\alpha_n)$ interseca H.

Caso 2: almeno uno degli α_i è trascendente su L. Sia per assurdo $\tau_1 G(\alpha_1) \cap \tau_2 G(\alpha_2) \cap \cdots \cap \tau_n G(\alpha_n) \cap H = \emptyset$. Siano $H_i = \{\tau \in G : \tau(\alpha_i) = \alpha_i\} \leq G$ per $i \in \{1, 2, \ldots, n\}$. Abbiamo che $G \setminus \tau_i G(\alpha_i) = \tau_i H_i$ e $H \subset \tau_1 H_1 \cup \cdots \cup \tau_n H_n$. Se per qualche i succede che $H \cap \tau_i H_i$ è contenuto nell'insieme $\bigcup_{j \neq i} \tau_j H_j$, allora se un elemento appartiene a $H \cap (\bigcap_{j \neq i} \tau_j G(\alpha_j))$ appartiene anche a $\tau_i G(\alpha_i)$. Dunque è sufficiente mostrare che

$H \cap (\bigcap_{j \neq i} \tau_j G(\alpha_j)) \neq \emptyset$. Iteriamo il procedimento finché non è più possibile omettere qualche $\tau_i G(\alpha_i)$. Se gli α_i rimasti sono algebrici su L allora il Caso 1 completa la dimostrazione. Dunque assumiamo ora che $H \subset \tau_1 H_1 \cup \cdots \cup \tau_n H_n$ dove nessun $\tau_i H_i$ può essere omesso e che uno degli α_i è trascendente su L. Assumiamo senza perdere di generalità che sia esso α_1. Allora il numero di possibili immagini distinte di α_1 per H è infinito. Per il Lemma 4.1 abbiamo che ponendo $H^1 = H_1 \cap \cdots \cap H_n$ allora $H \subset \bigcup_{k=1}^{p} t_k H^1$, un'unione di un numero finito p di classi laterali sinistre di H^1. Ora ogni elemento di H^1 fissa α_1. Se $h \in H$ allora $h = t_i h_1$, $h_1 \in H^1$ per qualche i. Dunque $h(\alpha_1) = t_i h_1(\alpha_1) = t_i(\alpha_1)$. Perció il numero di immagini distinte di α_1 per H è al massimo p. Questa è una contraddizione. Dunque ogni insieme aperto di base che contiene σ interseca H. Perció σ appartiene alla chiusura di H ma H è chiuso quindi $\sigma \in H$. Così ogni automorfismo di Ω su L appartiene ad H ed H è proprio il sottoinsieme di G che fissa L.

□

Esempio: Sia $\mathbb{C}(x)$ il campo delle funzioni razionali in una variabile su $\mathbb{C}$. Allora $\mathbb{C}(x)/\mathbb{C}$ è un'estensione di Galois trascendente, in particolare il suo gruppo di Galois è isomorfo al gruppo delle matrici invertibili 2x2 a coefficienti complessi $GL_2(\mathbb{C})$ modulo il sottogruppo delle matrici scalari $SC_2(\mathbb{C})$:

$$Gal(\mathbb{C}(x)/\mathbb{C}) \cong GL_2(\mathbb{C})/SC_2(\mathbb{C}).$$

Infatti dimostriamo inanzitutto che la mappa

$$GL_2(\mathbb{C}) \to Gal(\mathbb{C}(x)/\mathbb{C}),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \phi$$

con $\phi(x) = (ax+b)/(cx+d)$ e $ad - bc \neq 0$, è un omomorfismo di gruppi. Sia $\sigma \in Gal(\mathbb{C}(x)/\mathbb{C})$. Allora $\sigma(\mathbb{C}(x)) = \mathbb{C}(u)$ dove $u = \sigma(x)$. Poiché σ è un automorfismo, $\mathbb{C}(u) = \mathbb{C}(x)$ dunque $\sigma(x) = (ax+b)/(cx+d)$ per qualche $a, b, c, d \in \mathbb{C}$ con $ad - bc \neq 0$. Siano ora

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \phi \quad e \quad \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \mapsto \psi,$$

vogliamo mostrare che

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \mapsto \phi \circ \psi.$$

Notiamo che

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Abbiamo inoltre

$$\phi \circ \psi(x) = \frac{a(\frac{a'x+b'}{c'x+d'}) + b}{c(\frac{a'x+b'}{c'x+d'}) + d} = \frac{(aa' + bc')x + (ab' + bd')}{(ca' + dc')x + (cb' + dd')}$$

il che prova che $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \phi$ è un omomorfismo di gruppi. Supponiamo ora $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto id$. Allora $x = (ax+b)/(cx+d) \implies cx^2 + dx = ax + b \implies c = 0 = b$ e $a = d \implies A$ è una matrice scalare. Perciò il sottogruppo $SC_2(\mathbb{C}) \leq GL_2(\mathbb{C})$ delle matrici scalari è il Kernel della mappa $GL_2(\mathbb{C}) \to Gal(\mathbb{C}(x)/\mathbb{C})$. Dunque per il primo teorema di isomorfismo

$$GL_2(\mathbb{C})/SC_2(\mathbb{C}) \cong Gal(\mathbb{C}(x)/\mathbb{C}).$$

4.2 Proprietà della topologia di Soundararajan e Venkatachaliengar

Andiamo ora a vedere qualche proprietà della topologia $\mathcal{T}$ di Soundararajan e Venkatachaliengar, in particolare ci chiediamo quando essa risulti compatta. Scopriremo come ciò dipenda dal grado di trascendenza dell'estensione di Galois associata.

Teorema 4.4. Sia Ω/K un'estensione di Dedekind e sia G il gruppo di Galois di Ω su K. Consideriamo la topologia $\mathcal{T}$ su G introdotta nella Definizione 4.2. Allora $\mathcal{T}$ coincide con la topologia di Krull se e solo se Ω/K è un'estensione algebrica normale e separabile.

Il lemma seguente ci sarà utile per la dimostrazione del successivo Teorema 4.5

Lemma 4.2. Sia Ω un'estensione di K con grado di trascendenza finito. Allora la topologia $\mathcal{T}$ è compatta se e solo se è soddisfatta la seguenze condizione: se L è un campo intermedio di Ω/K tale che Ω è di Galois su L e $\bar{L}$ denota la chiusura algebrica di L su Ω allora un automorfismo di $\bar{L}$ su L può essere esteso ad un automorfismo di Ω su L.

Dimostrazione. Vedi [6, Theorem 4.3]. □

Teorema 4.5. Sia Ω/K un'estensione di Dedekind e sia G il gruppo di Galois di Ω su K. Consideriamo la topologia $\mathcal{T}$ su G introdotta nella Definizione 4.2. Se Ω ha grado di trascendenza finito , cioè $td_K(\Omega) < \infty$, allora $(G, \mathcal{T})$ è uno spazio compatto.

Dimostrazione. Sia L un campo intermedio di Ω/K e sia $\bar{L}$ la chiusura algebrica di L in Ω. Sia σ un automorfismo di $\bar{L}$ su L. Ora Ω ha grado di trascendenza finito anche su L. Sia $\{\alpha_1, \ldots, \alpha_r\}$ una base di trascendenza di Ω su L. Gli $\alpha_1, \ldots, \alpha_r$ sono algebricamente indipendenti anche su $\bar{L}$. Consideriamo il sottocampo $L(\alpha_1, \ldots, \alpha_r)$. Allora σ può essere esteso ad un automorfismo $\bar{\sigma}$ di $\bar{L}(\alpha_1, \ldots, \alpha_r)$ su $L(\alpha_1, \ldots, \alpha_r)$. Per ipotesi Ω è di Galois su $L(\alpha_1, \ldots, \alpha_r)$ ed è algebrica su $L(\alpha_1, \ldots, \alpha_r)$. Dunque Ω è un'estensione normale e separbile di $L(\alpha_1, \ldots, \alpha_r)$. Ora $L(\alpha_1, \ldots, \alpha_r) \leq \bar{L}(\alpha_1, \ldots, \alpha_r) \leq \Omega$ e $\bar{\sigma}$ è un automorfismo di $\bar{L}(\alpha_1, \ldots, \alpha_r)$ su $L(\alpha_1, \ldots, \alpha_r)$. Dunque $\bar{\sigma}$ può essere esteso ad un automorfismo σ_1 di Ω su $L(\alpha_1, \ldots, \alpha_r)$. La tesi è dimostrata grazie al Lemma 4.2. □

Proposizione 4.1. Sia Ω/K un'estensione di Dedekind e sia G il gruppo di Galois di Ω su K. Consideriamo la topologia $\mathcal{T}$ su G introdotta nella Definizione 4.2. $\mathcal{T}$ è la topologia meno fine su G per la quale:

a) i sottogruppi di G che fissano un'estensione intermedia sono $\mathcal{T}$-chiusi;

b) le traslazioni sono omeomorfismi.

Dimostrazione. Per il Teorema 4.3 i sottogruppi di G che fissano un'estensione intermedia sono $\mathcal{T}$-chiusi. Sia ora $\mathcal{J}$ una topologia su G per la quale valgano le proprietà a) e b). Mostriamo che $\mathcal{J}$ è più fine di $\mathcal{T}$, cioè che ogni insieme $\mathcal{T}$-aperto è $\mathcal{J}$-aperto. È sufficiente mostrare che $\tau G(\alpha)\rho$ è $\mathcal{J}$-aperto quando $G(\alpha) \neq \emptyset$. Poniamo $H_\alpha = \{\sigma \in G : \sigma(\alpha) = \alpha\}$, esso fissa un'estensione intermedia $K(\alpha)$ quindi è $\mathcal{J}$-chiuso. Dunque $G \setminus H_\alpha$ è $\mathcal{J}$-aperto ma $G \setminus H_\alpha = G(\alpha)$. Quindi anche $G(\alpha)$ è $\mathcal{J}$-aperto. Poichè la traslazione è un omeomorfismo per $(G, \mathcal{J})$, $\tau G(\alpha)$ è $\mathcal{J}$-aperto ed allo stesso modo $\tau G(\alpha)\rho$. □

Teorema 4.6. Sia Ω un'estensione algebricamente chiusa di K di caratteristica zero con grado di trascendenza infinito, cioè $td_K(\Omega) = \infty$. Sia G il gruppo di Galois di Ω su K. Allora non esiste alcuna topologia compatta $\mathcal{J}$ su G per la quale vi sia una corrispondenza di Galois tra i campi intermedi di Ω/K e i sottogruppi $\mathcal{J}$-chiusi di G.

Dimostrazione. Supponiamo che per assurdo esista una Topologia $\mathcal{J}$ che soddisfi le condizioni citate. La Proposizione 4.1 mostra che $\mathcal{J}$ è più fine di $\mathcal{T}$. Ma $\mathcal{J}$ è compatta. Dunque avremo che anche $\mathcal{T}$ è compatta. Ma ciò contraddice il teorema seguente: □

Teorema 4.7. Sia Ω un'estensione algebricamente chiusa di un campo K di caratteristica zero con grado di trascendenza infinito ($td_K(\Omega) = \infty$). Sia G il gruppo di Galois di Ω su K. Consideriamo la topologia $\mathcal{T}$ su G introdotta nella Definizione 4.2. Allora $\mathcal{T}$ non è compatta.

Dimostrazione. Sia B una base trascendente di Ω/K. Scriviamo $B = B_1 \cup B_2$, dove $B_1 \cap B_2 = \emptyset$ e sia $B_1 = \{\alpha_1, \alpha_2, \dots\}$ un insieme numerabile. Sia H il gruppo di Galois di Ω su $K(B_2)$ e per ogni i sia H_i il gruppo di Galois di Ω su $K(B_2, \alpha_i)$. Notiamo che $H_i \subset H$ e che i gruppi H_i, H sono $\mathcal{T}$-chiusi poichè fissano una certa estensione intermedia di Ω/K. Poiché Ω è un'estensione algebricamente chiusa di $K(B_2)$, per ogni i abbiamo un automorfismo σ_i di Ω/K tale che $\sigma_i(\alpha_i) = \alpha_{i+1}$, $\sigma_i(\alpha_{i+1}) = \alpha_i$, $\sigma_i(\alpha_j) = \alpha_j$, $\forall j \neq i, i+1$ e σ_i fissa ogni elemento di B_2. Dunque, poiché le traslazioni sono omeomorfismi per $\mathcal{T}$, $\sigma_i H_i$ è un'insieme chiuso. Consideriamo ora la collezione di insiemi chiusi $\{\sigma_i H_i\}$ per $i = 1, 2, \dots$.

(i) Questa collezione ha la proprietà dell'intesezione finita: consideriamo $\sigma_1 H_1 \cap \dots \cap \sigma_n H_n$. La mappa $\alpha_1 \mapsto \alpha_2$, $\alpha_2 \mapsto \alpha_3, \dots, \alpha_n \mapsto \alpha_{n+1}$, $\alpha_{n+1} \mapsto \alpha_1$, $\alpha_{n+j} \mapsto \alpha_{n+j}$ per $j = 2, 3, \dots$, $y \mapsto y$ $\forall y \in B_2$ produce un automorfismo di $K(B)$ su K e, poiché Ω è un estensione algebricamente chiusa di $K(B)$, può essere esteso ad un automorfismo σ di Ω su K. Affermiamo che $\sigma \in \sigma_1 H_1 \cap \dots \cap \sigma_n H_n$. Consideriamo H_i per $1 \leq i \leq n$ e l'automorfismo $\sigma_i^{-1}\sigma$. Poiché σ_i e σ fissano ogni elemento di B_2 abbiamo che $\sigma_i^{-1}\sigma$ fissa gli elementi di B_2. Inoltre $\sigma_i^{-1}\sigma(\alpha_i) = \sigma_i^{-1}(\alpha_{i+1}) = \alpha_i$. Ciò implica che $\sigma_i^{-1}\sigma \in H_i$ dunque $\sigma \in \sigma_i H_i$.

(ii) $\bigcap_{i=1}^{\infty} \sigma_i H_i = \emptyset$. Supponiamo per assurdo $\tau \in \bigcap_{i=1}^{\infty} \sigma_i H_i$. Allora $\tau \in H$ poiché $\sigma_i H_i \subset H$. Quindi τ è un automorfismo di Ω su $K(B_2)$. Inoltre per ogni i abbiamo

$\tau \in \sigma_i H_i$. Dunque $\sigma_i^{-1}\tau \in H_i$, cioè $\sigma_i(\alpha_i) = \tau(\alpha_i)$. Quindi $\tau(\alpha_i) = \alpha_{i+1}$ per ogni i. Sia ora $\bar{\alpha_1}$ la pre immagine di α_1 per l'automorfismo τ di Ω su $K(B_2)$. Allora $\bar{\alpha_1}$ è algebrico su $K(B)$. Dunque esiste una relazione algebrica che collega $\bar{\alpha_1}$ ed elementi di B con i coefficienti in K. Ora $\tau(\bar{\alpha_1}) = \alpha_1$ e $\tau(B) \subset B$. Applicando τ otteniamo una relazione algebrica che connette elementi di B. Questa è una contraddizione. Dunque vale $\bigcap_{i=1}^{\infty} \sigma_i H_i = \emptyset$.

(i) e (ii) mostrano che $\mathcal{J}$ non è compatta poiché esiste una famiglia di sottoinsiemi chiusi che ha la proprietà dell'intersezione finita ma ha intersezione vuota. □

Bibliografia

[1] D.J.H. Garling. *A Course In Galois Theory*, cap 18. Cambridge university press, 1986.

[2] I. Martin Isaacs. *Algebra: a graduate course*, cap 24. American Mathematical Society, 2009.

[3] J.S. Milne. *Fields and Galois Theory*, v5.10. 2022.

[4] J. Ruiter. *Infinite Galois Theory*. 2019. `file:///C:/Users/Utente/OneDrive/Documenti/UNIVERSITA'/III%20ANNO/LAUREA/TESI/Joshua%20Ruiter,%20Infinite%20Galois%20Theory.pdf`

[5] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*, pag. 141-143. Iwanami Shoten, 1971.

[6] T. Soundararajan, K. Venkatachaliengar. *Bulletin of the Australian Mathematical Society*, Volume 4, Issue 3, pag. 367-387. Cambridge University Press, 1971. `https://www.cambridge.org/core/services/aop-cambridge-core/content/view/1B344866687E31701BE9CE63D0907768/S0004972700046724a.pdf/on-the-krull-galois-theory-for-non-algebraic-extension-fields.pdf`

[7] Tamás Szamuely. *Galois Groups and Fundamental Groups*. Cambridge university press, 2009.