Elementi trascendenti ed indipendenza algebrica

Michele Placci

Sommario

Questa tesi è essenzialmente un lavoro di approfondimento, basato su argomenti inerenti la Teoria di Galois non trattati nell'omonimo corso affrontato in questa laurea.
Il lavoro è sviluppato in sei parti principali.
La prima di queste è una sezione puramente introduttiva, che vuole fornire una descrizione degli oggetti che saranno alla base di tutte le argomentazioni proposte. Nella seconda si entra già nell'argomento, con la distinzione tra elementi algebrici ed elementi trascendenti in un'estensione di campi. Questa si sviluppa in termini di mappe e si conclude con una generalizzazione che analizza sottoinsiemi algebricamente indipendenti. La terza riguarda le basi di trascendenza: si apre dandone una definizione, prosegue con le proprietà e termina con i teoremi numero sette e otto. Nella quarta, dopo l'analisi del teorema numero undici, si arriva a dare la definizione di grado di trascendenza, enunciandone alcune proprietà. Con la penultima parte, la quinta, si studia il rapporto tra i gradi di trascendenza in una torre di estensioni. La sesta infine, intitolata "Il teorema di Lüroth", risolve in un determinato caso, con questo teorema, il problema di determinare se un'estensione finitamente generata è puramente trascendente oppure no.
La trattazione si conclude con la dimostrazione della trascendenza del numero di Nepero, uno dei più conosciuti numeri reali trascendenti sul campo dei razionali.

1 Anello dei polinomi a coefficienti in un campo

Sia K campo. Indichiamo con $K[x]$ l'anello dei polinomi nell'indeterminata x a coefficienti in K ovvero

$$K[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid n \in \mathbb{N},\, a_0, \ldots, a_n \in K\}.$$

Analogamente con $K[x_1, \ldots, x_n]$ indichiamo l'anello dei polinomi in n indeterminate $x_1, \ldots, x_n$ a coefficienti in K. I suoi elementi si scrivono nella forma:

$$f = \textstyle\sum_{j=1}^{m} k_j x_1^{d_{1,j}} \cdots x_n^{d_{n,j}}$$

con $k_j \in K$ per $1 \leq j \leq m$ e $d_{i,j} \in \mathbb{N} \forall\ 1 \leq i \leq n, 1 \leq j \leq m$.

Con $K(x)$ denotiamo il campo delle frazioni di $K[x]$, cioè il campo delle funzioni razionali, quindi $K(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\, g(x) \neq 0\}$, mentre

$$K(x_1, \ldots, x_n) = \{\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g \neq 0\}.$$

Ora, sia $L \mid K$ estensione di campi, $\alpha, \alpha_1, \ldots, \alpha_n \in L$. Introduciamo la seguente notazione:
$K[\alpha] = \{a_0 + a_1\alpha + \ldots + a_n\alpha^n \mid n \in \mathbb{N}, a_i \in K\} = \{f(\alpha) \mid f(x) \in K[x]\} \subseteq L$
e $K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\} \subseteq L$.
Il campo delle frazioni di $K[\alpha]$ è $K(\alpha)$ dove:
$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(x)\,,\, g(x) \in K[x]\,,\, g(\alpha) \neq 0\}$ e il campo delle frazioni di $K[\alpha_1, \ldots, \alpha_n]$ è $K(\alpha_1, \ldots, \alpha_n) = \{\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f(x_1, \ldots, x_n)$,
$g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\ ,\ g(\alpha_1, \ldots, \alpha_n) \neq 0\}$.

Faremo uso nel seguito della *proprietà universale dell'anello dei polinomi:* Sia $L \mid K$ estensione di campi, $\alpha \in L$. Allora esiste un unico omomorfismo d'anelli $\varphi : K[x] \longmapsto L$ tale che φ ristretto a K è l'identità di K e $\varphi(x) = \alpha$. Spesso si indica tale φ con E_α, detta valutazione.

2 Elementi trascendenti ed indipendenza algebrica

Supponiamo che $L \mid K$ sia un'estensione e $\alpha \in L$. Allora ci sono due possibilità:

La 1^a: Esiste un polinomio $f(x) \in K[x]$, $f(x) \neq 0$, tale che $f(\alpha) = 0$ ovvero $\exists\ f = k_0 + k_1 x + \ldots + k_n x^n \in K[x], n \in \mathbb{N}$, tale che:
$f(\alpha) = k_0 + k_1\alpha + \ldots + k_n\alpha^n = 0$, cioè α è una radice di f. In questo caso si dice che α è *algebrico* su K.

La 2^a: Non esiste un tale poinomio in $K[x]$, e in questo caso α si dice *trascendente* su K . Tutto ciò può essere espresso in termini di mappe:
Consideriamo la valutazione E_α: $K[x] \longmapsto L$ tale che: $E_\alpha(f) = f(\alpha)$ per ogni $f \in K[x]$.
Allora:

$$\begin{aligned} \alpha \text{ è trascendente su } K &\iff E_\alpha \text{ è iniettiva} \\ \alpha \text{ è algebrico su } K &\iff E_\alpha \text{ non è iniettiva.} \end{aligned}$$

Infatti se α è trascendente su K, per quanto visto sopra, non esiste un polinomio non nullo di cui esso sia radice, quindi il nucleo di E_α è 0, ma allora E_α è un' iniezione.

Supponiamo che α sia algebrico su K. Allora $ker(E_\alpha) = K_\alpha$ è un ideale non vuoto di $K[x]$, e poichè $K[x]$ è un dominio a ideali principali, esiste un polinomio non nullo m_α tale che: $K_\alpha = (m_\alpha)$. Inoltre, poichè gli elementi invertibili di $K[x]$ sono tutti gli elementi diversi da zero di K, possiamo prendere m_α come polinomio monico, quindi m_α è del tipo: $m_\alpha = k_0 + k_1 x + \ldots + k_{n-1}x^{n-1} + x^n$.
Il polinomio m_α è detto il polinomio minimo per α, ed è univocamente determinato.
Vediamo due importanti teoremi:

Teorema 1 *Sia $L \mid K$ estensione, $\alpha \in L$ algebrico. Allora m_α è irriducibile in $K[x]$, l'immagine $E_\alpha(K[x])$ dell'anello dei polinomi $K[x]$ è il sottocampo $K(\alpha)$ di L e possiamo fattorizzare E_α con $i\widetilde{E}_\alpha q$, dove q è la mappa quoziente (epimorfismo canonico), $\widetilde{E}_\alpha$ è isomorfismo ed i la mappa inclusione.*

$$\begin{array}{ccc} K[x] & \xrightarrow{E_\alpha} & L \\ {\scriptstyle q}\downarrow & & \uparrow{\scriptstyle i} \\ K[x]/(m_\alpha) & \xrightarrow{\widetilde{E}_\alpha} & K(\alpha) \end{array}$$

Dimostrazione Supponiamo che $m_\alpha = f \times g$. Allora $0 = E_\alpha(m_\alpha) = E_\alpha(f) \times E_\alpha(g) = f(\alpha)g(\alpha)$. Quindi si ha che $f(\alpha) = 0$ o $g(\alpha) = 0$. Se $f(\alpha) = 0$, $f \in (m_\alpha)$ quindi $m_\alpha | f$ allora g è un'unità (elemento invertibile dell'anello $K[x]$). Analogamente se $g \in (m_\alpha)$, f è un'unità. Quindi m_α è irriducibile.
Dato che [1] un ideale $M = (p(x))$ di $K[x]$ è massimale se e solo se è irriducibile in K, e

Teorema 2 *Se R è anello commutativo con unità ed M ideale di R. M è ideale massimale di R se e solo se R/M è un campo.*

Possiamo concludere che $K[x]/(m_\alpha)$ è un campo.
Ora sappiamo che possiamo fattorizzare E_α nel seguente modo:

$$\begin{array}{ccc} K[x] & \xrightarrow{E_\alpha} & L \\ {\scriptstyle q}\downarrow & & \uparrow{\scriptstyle i} \\ K[x]/(m_\alpha) & \xrightarrow{\widetilde{E}_\alpha} & E_\alpha(K[x]) \end{array}$$

dove il primo teorema d'isomorfismo per anelli, garantisce che $\widetilde{E}_\alpha$ è un isomorfismo, quindi $E_\alpha(K[x])$ è sottocampo di L. Adesso poichè $E_\alpha(k) = k$ se $k \in K$ e $E_\alpha(x) = \alpha$ allora $E_\alpha(K[x]) \supseteq K(\alpha)$. Chiaramente $E_\alpha(K[x]) \subseteq K(\alpha)$, quindi la dimostrazione è conclusa. □

Teorema 3 *Sia $L \mid K$ estensione e $\alpha \in L$. Allora α è algebrico su K se e solo se $[K(\alpha) : K] < \infty$. In questo caso $[K(\alpha) : K]$ è il grado di m_α.*

Dimostrazione Per prima cosa supponiamo che $[K(\alpha) : K] = n < \infty$. Consideriamo i seguenti n+1 termini: $1, \alpha, \alpha^2, \ldots, \alpha^n \in K(\alpha)$. Se due termini α^r e α^s (con $0 \leq r < s \leq n$) sono uguali, $x^r - x^s$ appartiene al nucleo K_α della mappa E_α, oppure sono tutti distinti. In questo secondo caso, essendo n+1 termini, essi sono linearmente dipendenti su K. Quindi esistono $k_0, k_1, \ldots, k_n$ non tutti nulli elementi di K, tali che $k_0 + k_1\alpha + \ldots + k_n\alpha^n = 0$. Allora $f = k_0 + k_1x + \ldots + k_nx^n \in K_\alpha$, in ogni caso cioè E_α non è iniettiva, quindi α è algebrico su K. Supponiamo ora che α sia algebrico su K, e che m_α sia il polinomio minimo per α. Vogliamo mostrare che se $n = deg(m_\alpha)$, allora $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ formano una base per $K(\alpha)$ su K. Per prima cosa mostriamo che $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ è un insieme linearmente indipendente su K, infatti se $k_0 + k_1\alpha + \ldots + k_{n-1}\alpha^{n-1} = 0$ sia $f = k_0 + k_1x + \ldots + k_{n-1}x^{n-1}$.

Allora $f \in (K_\alpha) = (m_\alpha)$ e $deg(f) < deg(m_\alpha)$ ma allora $f = 0$, e $k_0 = k_1 = \cdots = k_{n-1} = 0$. In secondo luogo mostriamo che $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ è un insieme di generatori per $K(\alpha)$. Dal Teorema 1 se $b \in K(\alpha)$, allora $b = E_\alpha(f)$ per un certo $f \in K[x]$. Possiamo scrivere $f = m_\alpha \times q + r$ dove $r = 0$ o $deg(r) < n$. Allora $b = E_\alpha(f) = E_\alpha(m_\alpha)E_\alpha(q) + E_\alpha(r) = E_\alpha(r)$ allora se $r = k_0 + k_1 x + \ldots + k_{n-1}x^{n-1}$ si ha che $b = k_0 + k_1\alpha + \ldots + k_{n-1}\alpha^{n-1}$ quindi appartiene allo spazio generato da $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ □

Detto questo vediamo il seguente:

Teorema 4 *Supponiamo che $L \mid K$ sia un'estensione e che $\alpha \in L$ sia trascendente su K. Allora la mappa E_α può essere estesa in maniera unica ad un isomorfismo F_α dal campo $K(x)$ al campo $K(\alpha)$.*

Dimostrazione Sappiamo che il campo $K(x)$ è la collezione di tutte le classi d'equivalenza definite in $K[x] \times (K[x])^\star$ dalla relazione: $(r, s) \sim (r', s')$ se $rs' = r's$; dove appunto ogni classe è denotata da un'espressione della forma $\frac{r}{s}$ se (r, s) ne appartiene, quindi consideriamo $(f, g) \in K[x] \times (K[x])^\star$. Poichè α è trascendente su K, $g(\alpha) \neq 0$, e possiamo definire $G_\alpha(f, g) = f(\alpha)(g(\alpha))^{-1}$. Ora se $(f, g) \sim (f', g')$, $fg' = f'g$ in $K[x]$ quindi $f(\alpha)g'(\alpha) = f'(\alpha)g(\alpha)$ e $G_\alpha(f, g) = G_\alpha(f', g')$. Allora abbiamo che G_α è costante sulle classi di equivalenza, e possiamo perciò definire $F_\alpha(\frac{f}{g}) = G_\alpha(f, g)$. È chiaro che F_α è un omomorfismo d'anelli; inoltre poichè $F_\alpha(x) = E_\alpha(x) = \alpha$, $F_\alpha(K(x)) \supseteq K(\alpha)$.
D'altra parte se $\frac{f}{g} \in K(x)$, $F_\alpha(\frac{f}{g}) = \frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$, quindi $F_\alpha(K(x)) \subseteq K(\alpha)$, allora $F_\alpha(K(x)) = K(\alpha)$.

Infine se F'_α è un altro omomorfismo che estende E_α, l'insieme $R = \{r \in K(x) | F_\alpha(r) = F'_\alpha(r)\}$ è un sottocampo di $K(x)$ contenente $K[x]$, (perchè F_α ristretto a $K[x]$ è uguale a F'_α ristretto a $K[x]$). Esso deve perciò contenere l'intero $K(x)$, quindi F_α è unico. □

2.1 Sottoinsiemi algebricamente indipendenti

Suppniamo che $L \mid K$ sia un'estensione e che $A = \{\alpha_1, \ldots, \alpha_n\}$ sia un sottoinsieme finito di L con tutti gli elementi distinti. Ricordiamo che ogni elemento $f \in K[x_1, \ldots, x_n]$ può essere scritto nella forma:
$f = \sum_{j=1}^{m} k_j x_1^{d_{1,j}} \cdots x_n^{d_{n,j}}$
con $k_j \in K$ per $1 \leq j \leq m$ e $d_{i,j} \in \mathbb{N} \forall 1 \leq i \leq n, 1 \leq j \leq m$.
Consideriamo allora la mappa E_A da $K[x_1, \ldots, x_n]$ in L dove:
$E_A(f) = \sum_{j=1}^{m} k_j \alpha_1^{d_{1,j}} \cdots \alpha_n^{d_{n,j}}$. Scriveremo spesso $E_A(f)$ per $f(\alpha_1, \ldots, \alpha_n)$.
Diamo allora adesso la seguente definizione:

Definizione 1 *A è **algebricamente indipendente** su K se E_A è iniezione, cioè non esiste una relazione polinomiale a coefficienti in K tra gli elementi $\alpha_1, \ldots, \alpha_n$. Quindi il singoletto $\{\alpha\}$ è algebricamente indipendente su K se e solo se α è trascendente su K. Più in generale, diciamo che un arbitrario sottoinsieme S di L è algebricamente indipendente su K se ogni suo sottoinsieme finito è algebricamente indipendente su K.*

Il prossimo teorema è l'esatta generalizzazione del Teorema 4, è quindi omessa la dimostrazione:

Teorema 5 *Supponiamo che $L \mid K$ sia un'estensione e $A = \{\alpha_1, \ldots, \alpha_n\}$ sia algebricamente indipendente su K. Allora la mappa E_A può essere estesa in maniera unica all'isomorfismo F_A dal campo $K(x_1, \ldots, x_n)$ delle espressioni razionali in $x_1, \ldots, x_n$ al campo $K(\alpha_1, \ldots, \alpha_n)$.*

Analizziamo adesso un teorema molto importante che fornisce un criterio pratico per verificare se un insieme finito è algebricamente indipendente su K:

Teorema 6 *Supponiamo che $L \mid K$ sia un'estensione e che $\alpha_1, \ldots, \alpha_n$ siano distinti elementi di L. Sia $K_o = K$, $K_i = K(\alpha_1, \ldots, \alpha_i)$ per $1 \leq i \leq n$. Allora $A = \{\alpha_1, \ldots, \alpha_n\}$ è algebricamente indipendente su K se e solo se α_i è trascendente su K_{i-1}, per $1 \leq i \leq n$.*

Dimostrazione
($\Rightarrow$) Supponiamo che α_i sia algebrico su K_{i-1}. Allora
$f(\alpha_i) = k_0 + k_1\alpha_i + \ldots + k_r\alpha_i^r = 0$ per un certo $f \neq 0$ appartenente a $K_{i-1}[x] (= K(\alpha_1, \ldots, \alpha_{i-1})[x])$.
Possiamo scrivere ogni k_j come: $k_j = p_j(\alpha_1, \ldots, \alpha_{i-1})(q_j(\alpha_1, \ldots, \alpha_{i-1})^{-1})$ dove $p_j, q_j \in K[x_1, \ldots, x_{i-1}]$ e $q_j(\alpha_1, \ldots, \alpha_{i-1}) \neq 0$. Trasformiamo ora f in

un altro polinomio g a coefficienti in $K[x_1, \ldots, x_{i-1}]$:
Sia $l_j = p_j(\prod_{k \neq j} q_k)$ per $0 \leq j \leq r$.
Allora ogni $l_j \in K[x_1, \ldots, x_{i-1}]$ e $g = l_0 + l_1 x_i + \ldots + l_r x_i^r$ è un elemento diverso da zero di $K[x_1, \ldots, x_i]$.
Poichè $g(\alpha_1, \ldots, \alpha_i) = 0$, A non è algebricamente indipendente su K.

($\Leftarrow$) Supponiamo ora che $\{\alpha_1, \ldots, \alpha_n\}$ non sia algebricamente indipendente su K. Allora esiste un indice j tale che $\{\alpha_1, \ldots, \alpha_{j-1}\}$ è algebricamente indipendente su K, mentre $\{\alpha_1, \ldots, \alpha_j\}$ non lo è. Quindi esiste un $g \in K[x_1, \ldots, x_j],\ g \neq 0$, tale che $g(\alpha_1, \ldots, \alpha_j) = 0$.
Ragruppando i termini fra loro possiamo scrivere:
$g = k_0 + k_1 x_j + \ldots + k_r x_j^r$ dove $k_i \in K[x_1, \ldots, x_{j-1}]$ per $0 \leq i \leq r$.
Sia $h = k_0(\alpha_1, \ldots, \alpha_{j-1}) + k_1(\alpha_1, \ldots, \alpha_{j-1})x + \ldots + k_r(\alpha_1, \ldots, \alpha_{j-1})x^r$.
Abbiamo che $h \in K_{j-1}[x]$, e $h \neq 0$, perchè $\{\alpha_1, \ldots, \alpha_{j-1}\}$ è algebricamente indipendente su K. Poichè $h(\alpha_j) = 0$, α_j è algebrico su K_{j-1}. $\square$

3 Basi di trascendenza

Introduciamo adesso un'idea che corrisponde, sotto molti punti di vista, al concetto di base per uno spazio vettoriale.
Sia $L \mid K$ un'estensione ed $\mathcal{S}$ l'insieme di tutti i sottoinsiemi di L che sono algebricamente indipendenti su K. Ordiniamo $\mathcal{S}$ per inclusione. Un elemento S di $\mathcal{S}$ massimale in questo ordine è detto *base di trascendenza* per L su K.

Il prossimo risultato caratterizza le basi di trascendenza.

Teorema 7 *Supponiamo che $L \mid K$ sia un'estensione ed S un sottoinsieme di L. Allora S è una base di trascendenza per $L \mid K$ se e solo se S è algebricamente indipendente su K e $L \mid K(S)$ è algebrica.*

Dimostrazione Supponiamo che S sia una base di trascendenza per $L \mid K$, quindi per definizione algebricamente indipendente su K, e che α sia un elemento di L non appartenente ad S. Dalla condizione di massimalità rispettata da S segue che $S \cup \{\alpha\}$ non è algebricamente indipendente su K, quindi esistono distinti elementi $s_1, \ldots, s_n$ in S, e un $f \in K[x_0, \ldots, x_n], f \neq 0$, tali che: $f(\alpha, s_1, \ldots, s_n) = 0$. Possiamo scrivere f come: $k_0 + k_1 x_0 + \ldots + k_j x_0^j$ dove $k_i \in K[x_1, \ldots, x_n]$ per $0 \leq i \leq j$ e $k_j \neq 0$. Ora, poichè $\{s_1, \ldots, s_n\}$ è algebricamente indipendente su K concludiamo, primo che $j \geq 1$, secondo che $k_j(s_1, \ldots, s_n) \neq 0$. Adesso:
$k_0(s_1, \ldots, s_n) + k_1(s_1, \ldots, s_n)\alpha + \ldots + k_j(s_1, \ldots, s_n)\alpha^j = 0$
e poichè $k_i(s_1, \ldots, s_n) \in K(S)$ vuol dire che α è algebrico su $K(S)$ quindi $L \mid K(S)$ è algebrica.
Vediamo l'altra implicazione.
Supponiamo che S sia algebricamente indipendente su K e che $L \mid K(S)$ sia algebrica. Se $\alpha \in L \setminus S$, allora α è algebrico su $K(S)$, cioè esiste $g \neq 0$ con $g = k_0 + k_1 x + \ldots + k_j x^j$, $g \in K(S)[x]$ e tale che $g(\alpha) = 0$. Ogni coefficiente k_i coinvolge solo un numero finito di elementi di S, quindi esiste un sottoinsieme finito $\{s_1, \ldots, s_n\}$ di S tale che $k_i \in K(s_1, \ldots, s_n)$ per $0 \leq i \leq j$. Allora α è algebrico su $K(s_1, \ldots, s_n)$ e $\{s_1, \ldots, s_n, \alpha\}$ non è algebricamente indipendente su K, dal Teorema 6. Di conseguenza $S \cup \{\alpha\}$ non è algebricamente indipendente su K, ed S è cosi massimale; basta infatti aggiungere un solo elemento per far si che esso non sia più algebricamente indipendente su K. $\square$

Come ogni spazio vettoriale ha una base, così ogni estensione $L \mid K$ ha una base di trascendenza. Proviamo qualcosa di più:

Teorema 8 *Supponiamo che $L \mid K$ sia un'estensione e che A sia un sottoinsieme di L tale che $L \mid K(A)$ sia algebrica e C un sottoinsieme di A che sia algebricamente indipendente su K. Allora esiste una base di trascendenza B per L su K con $C \subseteq B \subseteq A$.*

Osservazione 1 *Prendendo $A = L$ e C vuoto, questo teorema assicura che ogni estensione ha una base di trascendenza.*

Dimostrazione Per dimostrarlo ci servirà il *lemma di Zorn*. Ricordiamo quindi che: un sottoinsieme non vuoto C di un insieme parzialmente ordinato S è una *catena,* se è totalmente ordinato dalla relazione d'ordine indotta da S.
Lemma di Zorn: Supponiamo che S sia un insieme parzialmente ordinato, con la proprietà che ogni catena di abbia un maggiorante. Allora S ha almeno un elemento massimale.
Allora sia S l'insieme dei sottoinsiemi di A che sono algebricamente indipendenti e contenenti C. Ordiniamo S per inclusione. Supponiamo che T sia una catena di S e sia $E = \bigcup_{D \in T} D$. Quindi E è un sottoinsieme di A contenente C. Supponiamo che $x_1, \ldots, x_n$ siano distinti elementi di E. Dalla definizione di E esistono n insiemi $D_1, \ldots, D_n$ in T tali che $x_i \in D_i$ per $1 \leq i \leq n$. Poichè T è una catena, esiste un indice j, con $1 \leq j \leq n$, tale che $D_i \subseteq D_j$ per $1 \leq i \leq n$. Di conseguenza $x_1, \ldots, x_n$ appartengono tutti a D_j. Essendo D_j algebricamente indipendente, $\{x_1, \ldots, x_n\}$ è algebricamente indipendente. Poiché tutto questo è vero per ogni sottoinsieme finito di E, E è algebricamente indipendente.
Allora $E \in S$, ed E è chiaramente un maggiorante per T, quindi ogni catena in S ha un maggiorante. Possiamo allora applicare il lemma di Zorn e concludere che S ha un elemento massimale B.
Quindi B è algebricamente indipendente e $C \subseteq B \subseteq A$.
Per concludere la dimostrazione, in base al Teorema 7, dobbiamo mostrare che $L \mid K(B)$ è algebrica. Per fare ciò vediamo prima altri due teoremi:

Teorema 9 *Sia $L \mid K$ un'estensione. Le seguenti affermazioni sono equivalenti:*

- (i) $[L : K] < \infty$;
- (ii) *$L \mid K$ è algebrica, e L è finitamente generato su K;*
- (iii) *esiste un numero finito di elementi algebrici $\alpha_1, \ldots, \alpha_n \in L$ tali che $L = K(\alpha_1, \ldots, \alpha_n)$.*

Dimostrazione Supponiamo per prima cosa che $L \mid K$ sia finita. Se $\alpha \in L$ allora $[K(\alpha) : K] \leq [L : K] < \infty$ allora α è algebrico su K (per il Teorema 3, pag 7), quindi $L \mid K$ è algebrica. Ora se $(\beta_1, \ldots, \beta_r)$ è una base per L su K, allora $L = K(\beta_1, \ldots, \beta_r)$, quindi L è finitamente generato su K. Allora $(i) \Rightarrow (ii)$ e certamente $(ii) \Rightarrow (iii)$. Supponiamo adesso che valga (iii). Sia $K_0 = K$ e sia $K_j = K(\alpha_1, \ldots, \alpha_j) = K_{j-1}(\alpha_j)$, per $1 \leq j \leq n$. Si noti che $L = K_n$. Ogni α_j è algebrico su K_{j-1} quindi $[K_j : K_{j-1}] < \infty$. Abbiamo una torre di estensioni, e di conseguenza:
$[L : K] = [K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_1 : K_0] < \infty$. □

Corollario 1 *Se $L \mid K$ è un'estensione e α un elemento di L algebrico su K, allora $K(\alpha) \mid K$ è algebrica.*

Questo è un caso particolare del seguente:

Corollario 2 *Sia $L \mid K$ estensione e $S \subset L$. Se ogni $\alpha \in S$ è algebrico su K, allora $K(S) \mid K$ è algebrica.*

Dimostrazione Se $\beta \in K(S)$, allora esistono $\alpha_1, \ldots, \alpha_n \in S$ tali che $\beta \in K(\alpha_1, \ldots, \alpha_n)$. Dal Teorema 9, $K(\alpha_1, \ldots, \alpha_n) \mid K$ è algebrica, quindi β è algebrico su K. □

La dimostrazione di questo corollario mostra che, sebbene un' estensione algebrica possa essere infinita, è possibile occuparsi di essa usando argomenti che coinvolgono estensioni finite. Lo stesso vale per il prossimo teorema:

Teorema 10 *Siano $M \mid L$ e $L \mid K$ estensioni algebriche. Allora $M \mid K$ è estensione algebrica.*

Dimostrazione Sia $\alpha \in M$ e $m_\alpha = l_0 + l_1 x + \ldots + l_{n-1}x^{n-1} + x^n$ il suo polinomio minimo su L. Allora α è algebrico su $K(l_0, \ldots, l_{n-1})$ quindi:
$[K(l_0, \ldots, l_{n-1})(\alpha) : K(l_0, \ldots, l_{n-1})] = [K(l_0, \ldots, l_{n-1}, \alpha) : K(l_0, \ldots, l_{n-1})] < \infty$
(dal Teorema 3, pag 7). Anche $[K(l_0, \ldots, l_{n-1}) : K] < \infty$ perché per ipotesi $L \mid K$ è algebrica e vale il teorema 9.
Allora: $[K(\alpha) : K] \leq [K(l_0, \ldots, l_{n-1}, \alpha) : K] = \ldots$
$\ldots = [K(l_0, \ldots, l_{n-1}, \alpha) : K(l_0, \ldots, l_{n-1})] \cdot [K(l_0, \ldots, l_{n-1}) : K] < \infty$. Quindi α è algebrico su K. □

Vediamo ora come si conclude la dimostrazione al teorema 8.
Sappiamo che ogni elemento $\alpha \in A$ è algebrico su $K(B)$. Allora $K(A) \mid K(B)$ è algebrica grazie al corollario 2 al Teorema 9. Poiché per ipotesi $L \mid K(A)$ è algebrica allora $L \mid K(B)$ è algebrica (Teorema 10), così B è base di trascendenza per $L \mid K$, essendo soddisfatte tutte le condizioni del Teorema 7.
□

Osservazione 2 *Consideriamo l'estensione $\mathbb{R}/\mathbb{Q}$. Se S è un sottoinsieme numerabile di $\mathbb{R}$, $\mathbb{Q}(S)$ è numerabile. Se $\mathbb{R}/\mathbb{Q}(S)$ fosse algebrica, $\mathbb{R}$ sarebbe numerabile, quindi ogni base di trascendenza per $\mathbb{R}$ su $\mathbb{Q}$ deve essere non numerabile.*

Osservazione 3 *Si noti anche che, da questo Teorema 8, se $L \mid K$ è finitamente generata su K, allora deve esserci una base di trascendenza finita per $L \mid K$. Infatti se nel teorema si pone come A, l'insieme finito di questi generatori, come risultato otteniamo l'esistenza della base di trascendenza B appunto contenuta in A perciò anch'essa finita.*

4 Il grado di trascendenza

Teorema 11 *Supponiamo che $L \mid K$ sia un'estensione, che $C = \{c_1, \ldots, c_r\}$ sia un sottoinsieme di L, di r distinti elementi, algebricamente indipendente su K, e che $A = \{a_1, \ldots, a_s\}$ sia un sottoinsieme di L, con s distinti elementi, tale che $L \mid K(A)$ sia algebrica. Allora $r \leq s$, ed esiste un insieme D, con $C \subseteq D \subseteq A \cup C$ tale che $\mid D \mid = s$ e $L \mid K(D)$ è algebrica.*

Dimostrazione Per induzione su r. Se $r = 0$ basta prendere $D = A$. Supponiamo sia vero per $r-1$. Quindi con $C_0 = \{c_1, \ldots, c_{r-1}\}$ algebricamente indipendente su L, esiste un insieme D_0 con: $C_0 \subseteq D_0 \subseteq A \cup C_0$ tale che $\mid D_0 \mid = s$ e $L \mid K(D_0)$ è algebrica. Rienumerando gli indici di A se necessario, possiamo supporre

$$D_0 = \{c_1, \ldots, c_{r-1}, a_r, a_{r+1}, \ldots, a_s\}.$$

Poichè $L \mid K(D_0)$ è algebrica, c_r è algebrico su $K(D_0)$. Essendo $\{c_1, \ldots, c_r\}$ algebricamente indipendente su K, c_r è trascendente su $K(c_1, \ldots, c_{r-1})$. Quindi $s \geq r$. Ancora dal Teorema 6 abbiamo che:

$$E = \{c_1, \ldots, c_{r-1}, c_r, a_r, a_{r+1}, \ldots, a_s\}$$

è algebricamente dipendente su K. Sfruttando il Teorema 6 ancora una volta, e usando il fatto che $\{c_1, \ldots, c_r\}$ è algebricamente indipendente su K, concludiamo che deve esistere un t, con $r \leq t \leq s$, tale che a_t sia algebrico su $K\{c_1, \ldots, c_r, a_r, \ldots, a_{t-1}\}$. Sia $D = \{c_1, \ldots, c_r, a_r, \ldots, a_{t-1}, a_{t+1}, \ldots, a_s\}$, allora a_t è algebrico su $K(D)$, quindi $K(E) \mid K(D)$ è algebrica. Poichè $E \supseteq D_0$, $L \mid K(E)$ è algebrica, ma allora $L \mid K(D)$ è algebrica, dal Teorema 10. Poichè $C \subseteq D \subseteq A \cup C$ e $\mid D \mid = s$, la dimostrazione è completata. □

Corollario 3 *Se $L \mid K$ è un'estensione ed S e T sono due basi di trascendenza per $L \mid K$, allora o entrambe S e T sono infinite, oppure S e T hanno lo stesso finito numero di elementi.*

Se un'estensione $L \mid K$ ha una base di trascendenza finita, si definisce *grado di trascendenza* dell'estensione il numero di elementi della base di trascendenza. In caso contrario diremo che il grado di trascendenza di $L \mid K$ è infinito.

5 Altre proprietà del grado di trascendenza

Supponiamo che $M \mid L$ e $L \mid K$ siano estensioni. Qual è il grado di trascendenza di $M \mid K$ in relazione ai gradi di trascendenza di $M \mid L$ e $L \mid K$?

Teorema 12 *Supponiamo che $M \mid L$ e $L \mid K$ siano estensioni, che A sia un sottoinsieme di L algebricamente indipendente su K, e che B sia un sottoinsieme di M algebricamente indipendente su L. Allora $A \cup B$ è algebricamente indipendente su K.*

Dimostrazione Sia C sottoinsieme finito di $A \cup B$. Possiamo scrivere $C = \{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ con $\alpha_i \in A$, $\beta_j \in B$.
Dal Teorema 6, α_i è trascendente su $K(\alpha_1, \ldots, \alpha_{i-1})$ per $1 \leq i \leq r$ e β_j è trascendente su $L(\beta_1, \ldots, \beta_{j-1})$ per $1 \leq j \leq s$, quindi β_j è trascendente su $K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_{j-1})$ per $1 \leq j \leq s$. Allora C è algebricamente indipendente su K, sempre per il Teorema 6. Poichè questo è vero per ogni sottoinsieme finito di $A \cup B$, $A \cup B$ è algebricamente indipendente su K. □

Questo teorema ci sarà utile nel seguente:

Teorema 13 *Supponiamo che $M \mid L$ e $L \mid K$ siano estensioni, che A sia una base di trascendenza per $L \mid K$ e che B sia una base di trascendenza per $M \mid L$. Allora $A \cup B$ è una base di trascendenza per $M \mid K$.*

Dimostrazione Dai teoremi 7 e 12, è sufficiente mostrare che $M \mid K(A \cup B)$ è algebrica. Poichè A è una base di trascendenza per $L \mid K$, $L \mid K(A)$ è algebrica. Poichè $K(A) \subseteq K(A \cup B)$, segue che $K(A \cup B)(L) \mid K(A \cup B)$ è algebrica. Essendo $K(A \cup B)(L) = L(B)$, segue che $L(B) \mid K(A \cup B)$ è algebrica. Ma B è una base di trascendenza per $M \mid L$, quindi $M \mid L(B)$ è algebrica. In conclusione $M \mid K(A \cup B)$ è algebrica dal Teorema 10. □

Corollario 4 *Se $M \mid L$ e $L \mid K$ sono estensioni, il grado di trascendenza di $M \mid K$ è dato dalla somma dei gradi di trascendenza di $M \mid L$ e $L \mid K$.*

Dimostrazione Per il Teorema appena visto, basta far vedere che $A \cap B = \emptyset$, ma questo è ovvio perchè ogni $\beta \in B$ è trascendente su $K(A)$. □

6 Il teorema di Lüroth

Supponiamo che $L \mid K$ sia un'estensione finitamente generata con grado di trascendenza r. Se $\alpha_1, \ldots, \alpha_r$ è una base di trascendenza per $L \mid K$, allora $L \mid K(\alpha_1, \ldots, \alpha_r)$ è estensione finita.
Se è possibile trovare una base di treascendenza $\alpha_1, \ldots, \alpha_r$ per $L \mid K$ tale che $L = K(\alpha_1, \ldots, \alpha_r)$, allora si dice che L è *puramente trascendente* su K.
Anche in casi particolari 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 teorema [2] più un suo corollario, che ci saranno poi utili nella dimostrazione.

Teorema 14 *Se R è un dominio a fattorizzazione unica, tale è $R[x]$.*

Corollario 5 *Supponiamo che f sia un elemento primitivo di $R[x]$, e che g sia un elemento di $R[x]$ con $g \neq 0$. Se f divide g in $F[x]$, con F il campo delle frazioni di R, allora f divide g in $R[x]$.*

Dimostrazione Possiamo fattorizzare g come

$g = \alpha_1 \cdot \ldots \cdot \alpha_j g_1 \cdot \ldots \cdot g_k$ dove gli α_i sono irriducibili di R e i g_i sono elementi irriducibili di $R[x]$ di grado positivo. Dal lemma di Gauss, ogni g_i è primitivo e irriducibile in $F[x]$. Quindi $g = (\alpha_1 \cdot \ldots \cdot \alpha_j g_1) g_2 \cdot \ldots \cdot g_k$ è una fattorizzazione di g come prodotto di irriducibili di $F[x]$. Poichè f divide g in $F[x]$ ed essendo $F[x]$ un dominio a fattorizzazione unica, possiamo scrivere

$f = \varepsilon g_{i_1} \cdot \ldots \cdot g_{i_r}$

dove $\varepsilon \neq 0$, $\varepsilon \in F$ e $1 \leq i_1 < \ldots < i_r \leq k$. Ora $g_{i_1} \cdot \ldots \cdot g_{i_r}$ è primitivo, perchè prodotto di primitivi e poichè f è anch'esso primitivo, ε è un'unità di R, quindi f divide g in $R[x]$. □

Vediamo allora il **Teorema di Lüroth**

Teorema 15 *Supponiamo che $K(t) \mid K$ sia un'estensione semplice, e che t sia trascendente su K. Se L è un sottocampo di $K(t)$ contenente K, allora $L \mid K$ è un'estensione semplice.*

Dimostrazione Chiaramente ci basta considerare il caso in cui L sia diverso da K e da $K(t)$. Se $s \in L \setminus K$, possiamo scrivere $s = p(t)/q(t)$ dove p e q sono polinomi non nulli di $K[x]$. Allora $q(t)s - p(t) = 0$, e t è algebrico su L. Sia m il polinomio minimo per t su L. Possiamo considerare m come un elemento di $K(t)[x]$. Allora esiste un $\beta \in K(t)$ tale che $\beta m = f$, dove

$f = a_0(t) + a_1(t)x + \ldots + a_n(t)x^n$
è un polinomio primitivo di $K[t][x]$. Si noti che: $n = deg(m) = [K(t) : L]$. Poichè m è monico, $\beta = a_n(t)$ e i termini $\frac{a_i(t)}{a_n(t)}$ appartengono tutti ad L; d'altra parte, essi non appartengono tutti a K, perchè t è trascendente su K. Esiste perciò un i, con $0 \leq i < n$, tale che $u = \frac{a_i(t)}{a_n(t)} \in L \setminus K$. Possiamo scrivere u come $\frac{g(t)}{h(t)}$ dove g ed h sono polinomi relativamente primi fra loro in $K[t]$.
Sia $r = max(deg(g), deg(h))$. Allora $[K(t) : K(u)] = r$.
(Infatti se $u = \frac{g(t)}{h(t)} \Rightarrow u\frac{h(t)}{g(t)} = 1 \Rightarrow \frac{uh(t)-g(t)}{g(t)} = 0 \Rightarrow uh(t) - g(t) = 0$ e $deg(uh - g) = max(deg(g), deg(h)))$. Poichè $K(u) \subseteq L$, questo significa che $r \geq n$. Ma vuol dire anche che è sufficiente mostrare che $r \leq n$ per concludere che $L = K(u)$.

Consideriamo ora la seguente espressione:

$l = g(t)h(x) - h(t)g(x).$

Poichè g ed h sono relativamente primi, $l \neq 0$.
Ora $(h(t))^{-1}l \in L[x]$, e $(h(t))^{-1}l$ ha t come radice, quindi m divide $(h(t))^{-1}l$ in $L[x]$. Questo implica che f divide l in $K(t)[x]$. Essendo poi f primitivo in $K[t][x]$, segue dall'ultimo teorema visto che f divide l in $K[t][x]$. Quindi esiste $j \in K[t][x]$ tale che $l = fj$. Possiamo considerare f, l e j sia come elementi di $K[t][x]$ che come elementi di $K[x][t]$: denotiamo allora con deg_x il grado in x, e con deg_t il grado rispetto a t.
Ora $deg_t(l) \leq r$ e $deg_t(f) \geq r$: poichè $l = fj$, $deg_t(l) = deg_t(f) = r$, e $deg_t(j) = 0$. In altre parole possiamo considerare j come un elemento di $K[x]$. In particolare, questo significa che j è primitivo in $K[t][x]$, quindi l, essendo il prodotto di f e j, è primitivo in $K[t][x]$. Poichè l è simmetrico in t e x, questo implica che l è primitivo in $K[x][t]$. Ma $j \in K[x]$ e j divide l, quindi j deve essere un'unità di $K[x]$ cioè $j \in K$. Di conseguenza
$n = deg_x(f) = deg_x(l) = deg_t(l) = deg_t(f) \geq r$
e la dimostrazione è conclusa. □

A La trascendenza di e

Teorema 16 *e è trascendente su* $\mathbb{Q}$

Dimostrazione Per assurdo sia $a_m e^m + a_{m-1}e^{m-1} + \ldots + a_1 e + a_0 = 0$ con $a_i \in \mathbb{Z}\ \forall\ 0 \leq i \leq m$.
Scegliamo un primo $p \in \mathbb{Z}$, $p > m$, $p > a_0$ e consideriamo il seguente polinomio[1]

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-m)^p}{(p-1)!} \in \mathbb{Q}[x]$$

$deg(f) = \delta f = mp + p - 1$.

Sia $F(x) = f + f^{(1)} + f^{(2)} + \ldots + f^{(\delta f)} \in \mathbb{Q}[x]$,
allora $F^{(1)}(x) = F(x) - f(x)$.
Ora calcoliamo $\frac{d}{dx}[e^{-x}F(x)] = -e^{-x}F(x) + e^{-x}F^{(1)}(x) = -e^{-x}f(x)$
quindi con $i = 1, 2, \ldots, m$ (ne fissiamo uno),

$$\int_0^i \frac{d}{dx}[e^{-x}F(x)]dx \ = \ -\int_0^i e^{-x}f(x)dx \ = \ e^{-i}F(i) - F(0).$$

Adesso

$$\begin{aligned}
-e^i \int_0^i e^{-x}f(x)dx &= F(i) - e^i F(0) \\
-a_i e^i \int_0^i e^{-x}f(x)dx &= a_i F(i) - a_i e^i F(0) \\
-\sum_{i=0}^m a_i e^i \int_0^i e^{-x}f(x)dx &= \sum_{i=0}^m a_i F(i) - F(0)[\sum_{i=0}^m a_i e^i] = \sum_{i=0}^m a_i F(i)
\end{aligned}$$

perchè $\sum_{i=0}^m a_i e^i = 0$ per l'ipotesi assurda iniziale.
Allora abbiamo ottenuto che:

$$-\sum_{i=0}^m a_i e^i \int_0^i e^{-x}f(x)dx \ = \ \sum_{i=0}^m a_i F(i).$$

Adesso dimostreremo che il primo membro tende a 0 per p tendente all'infinito, mentre il secondo membro è comunque un intero diverso da zero, e

[1] Usato per la prima volta da Hermite, (1873) nella prima dimostrazione della trascendenza del numero di Nepero.

non può quindi essere infinitesimo. Iniziamo da questo secondo fatto:

$$\begin{aligned}\sum_{i=0}^{m} a_i F(i) &= a_0F(0) + a_1F(1) + \ldots + a_mF(m) \\ &= a_0(f(0) + f^{(1)}(0) + \ldots + f^{(\delta f)}(0)) + a_1(f(1) + \ldots + f^{(\delta f)}(1)) + \ldots \\ &\quad \ldots + a_m(f(m) + \ldots + f^{(\delta f)}(m)).\end{aligned}$$

Allora

$f^{(j)}(i)$ per $0 \leq j \leq (p-2)$ e $0 \leq i \leq m$ è nullo,
come è nullo $f^{(p-1)}(k)$ per $1 \leq k \leq m$
mentre $f^{(p-1)}(0) = (-1)^m(m!)^p$
infine $f^{(t)}(i)$ per $p \leq t \leq (\delta f)$ e $0 \leq i \leq m$ da sempre come risultato un multiplo di p.

Quindi in conclusione $\sum_{i=0}^{m} a_i F(i) = a_0(-1)^m(m!)^p + pz_0$ per un opportuno $z_0 \in \mathbb{Z}$

Ma $a_0(-1)^m(m!)^p + pz_0$ non sarà mai nullo, perchè ciò vorrebbe dire che $a_0(-1)^m(m!)^p = pz_0$, con i segni opportuni, quindi $a_0(-1)^m(m!)^p$ sarebbe un multiplo di p cioè divisibile per p, che essendo primo dovrebbe necessariamente dividere a_0 oppure $(m!)^p$. Ma per ipotesi abbiamo posto $p > m, a_0$.

Passiamo adesso alla dimostrazione che il secondo membro è infinitesimo per $p \to \infty$.
Abbiamo

$$-\sum_{i=0}^{m} a_i e^i \int_0^i e^{-x} f(x)dx.$$

Prendiamo in considerazione l'integrale

$$\int_0^i e^{-x} f(x)dx.$$

Dal teorema del valor medio ($\int_a^b f(x)dx = (b-a)f(x_0)$ con $a \leq x_0 \leq b$) si ha che

$$\int_0^i e^{-x} f(x)dx = ie^{-\xi} f(\xi) \text{ con } 0 \leq \xi \leq i.$$

Ora:

$$f(\xi) = \frac{\xi^{p-1}(\xi-1)^p \cdots (\xi-m)^p}{(p-1)!} < \frac{m^{p-1}m^p \cdots m^p}{(p-1)!} = \cdots$$
$$\cdots = \frac{m^{pm+p-1}}{(p-1)!} = \frac{m^{(m+1)(p-1)+m}}{(p-1)!} = m^m \frac{N^{p-1}}{(p-1)!}$$

con $N = m^{m+1}$
dove $\frac{N^{p-1}}{(p-1)!} \to 0$ per $p \to \infty$ (Perchè sappiamo che $e^N = \sum_{i=0}^{\infty} \frac{N^i}{i!} = \sum_{i=1}^{\infty} \frac{N^{i-1}}{(i-1)!}$ dove la frazione va a zero, altrimenti non c'è convergenza).

Abbiamo così ottenuto una contraddizione al fatto che il secondo membro è invece un intero non infinitesimo. □

Riferimenti bibliografici

[1] I. N. Herstein, *Algebra*, Editori Riuniti, Roma (1999).

[2] D. J. H. Garling, *A course in Galois theory*, Cambridge University, press in New York (1986).

Indice