Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Estensioni trascendenti

Relatore:
Prof. Riccardo Colpi

Laureando: Eleonora Bedin
Matricola: 2035015

Anno Accademico 2024/2025

25/07/2025

Indice

Introduzione **5**

1 Estensioni di campi **7**
1.1 Nozioni preliminari 7

2 Estensioni trascendenti **11**
2.1 Indipendenza algebrica 11
2.2 Basi di trascendenza 16
2.3 Grado di trascendenza 18
2.3.1 I polinomi simmetrici elementari 21
2.4 Teorema di Lüroth 22
2.5 Basi di trascendenza separanti 26

3 I numeri trascendenti **27**
3.1 Accenni storici 27
3.2 I numeri di Liouville 28
3.3 L'esistenza dei numeri trascendenti 29

4 La trascendenza di e e π **31**
4.1 Trascendenza di e 32
4.2 Trascendenza di π 34
4.3 Indipendenza algebrica di e e π 36

Introduzione

Lo scopo di questo elaborato è lo studio delle estensioni trascendenti, in particolare della loro struttura e dei concetti fondamentali che ne stanno alla base. Nel corso della trattazione verranno presentati diversi risultati che hanno segnato in maniera rilevante il processo di ricerca in questo ambito, accompagnati da esempi volti a rendere più chiaro e accessibile l'argomento.

Nel primo capitolo verranno introdotti gli strumenti e le nozioni necessarie alla comprensione dei capitoli successivi. Si forniranno quindi una serie di definizioni fondamentali, tra cui quelle di elemento algebrico e di elemento trascendente. Questi ultimi hanno una stretta correlazione con i concetti che verranno formalizzati in seguito.

Nel secondo capitolo verranno presentati il concetto di dipendenza e indipendenza algebrica, e le proprietà che caratterizzano le estensioni trascendenti. Si introdurrà la nozione di base di trascendenza, ponendo particolare attenzione alla relazione con gli insiemi algebricamente indipendenti. In seguito, dopo aver descritto la nozione di grado di trascendenza e di estensione puramente trascendente, si approfondirà il ruolo dei polinomi simmetrici elementari, che costituiscono un esempio significativo di base di trascendenza. Tali nozioni saranno propedeutiche alla dimostrazione del Teorema di Luröth, utile a verificare in maniera immediata se un'estensione finitamente generata sia puramente trascendente. Infine si descriverà il concetto di basi di trascendenza separanti.

Il terzo capitolo è dedicato alla storia della teoria dei numeri trascendenti e a come Joseph Liouville, Charles Hermite, Ferdinand von Lindemann e Georg Cantor contribuirono allo sviluppo della matematica in questo campo. In particolare, verranno analizzati i numeri di Liouville e, utilizzando diverse nozioni provenienti dalla teoria degli insiemi, si dimostrerà l'esistenza dei numeri trascendenti.

Nel quarto capitolo verranno introdotti il Teorema di Hermite e il Teorema di Lindemann, che condussero rispettivamente alla dimostrazione della trascendenza del numero di Nepero e di Pi greco. Dopo aver presentato una ulteriore dimostrazione diretta di tali risultati, si discuteranno diverse proprietà che caratterizzano i numeri trascendenti, applicandole in particolare a e e π. Infine si farà riferimento all'indipendenza algebrica di e e π, richiamando la Congettura di Schanuel. Quest'ultima, se verificata, potrebbe condurre a sviluppi significativi nella teoria dei numeri trascendenti .

Capitolo 1

Estensioni di campi

1.1 Nozioni preliminari

In questo capitolo introduttivo richiamiamo alcune definizioni e proprietà nell'ambito della teoria dei campi, preliminari ai contenuti di questo elaborato.

Definizione 1.1.1. (Estensione di un campo). Un campo Ω si definisce *estensione di un campo* F se contiene F come sottocampo. Tale contesto si denota con il simbolo Ω/F.

In tal caso Ω è in modo naturale un F-spazio vettoriale. Pertanto è ben posta la seguente:

Definizione 1.1.2. (Grado di un'estensione). Sia Ω/F un'estensione di campi. La dimensione di Ω come spazio vettoriale su F si chiama *grado* di Ω su F e si denota con $[\Omega : F]$. Ω si dice *estensione finita* di F quando tale grado è finito, in caso contrario si dice *infinita*.

Proposizione 1.1.3. (Formula dei gradi) Siano $F \subseteq \Omega \subseteq M$ campi. Allora $[M : F] = [M : \Omega][\Omega : F]$.

Dimostrazione. Il fatto è ovvio se $[M : \Omega] = \infty$ oppure $[\Omega : F] = \infty$ (qui adottiamo la convenzione $\infty \cdot n = \infty$).
Quindi assumiamo che $[M : \Omega] = n$ e $[\Omega : F] = m$ siano entrambi finiti. Sia $\{a_1, \ldots, a_n\}$ una base di M su Ω, e sia $\{b_1, \ldots, b_m\}$ una base di Ω su F. Proviamo che gli elementi $\{b_j a_i\}_{1 \leq j \leq m, 1 \leq i \leq n}$ costituiscono una base di M su F. Dato $u \in M$ esistono $x_1, x_2 \ldots, x_n$ in Ω tali che $u = \sum_{i=1}^{n} x_i a_i$. Ogni $x_i \in \Omega$ è a sua volta una combinazione a coefficienti in F della base

$\{b_1, \ldots, b_m\}$: $x_i = \sum_{j=1}^{m} y_{ji} b_j$. Quindi possiamo scrivere:

$$u = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i)$$

Abbiamo trovato che ogni $u \in M$ è combinazione a coefficienti in F degli elementi $b_j a_i$.
Proviamo ora che il sistema $\{b_j a_i\}_{i,j}$ è linearmente indipendente.
Sia $\sum y_{ji} b_j a_i = 0$ con $y_{ji} \in F$. Possiamo riscrivere nel modo seguente:

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i$$

Poiché i termini a_i sono linearmente indipendenti su Ω, si ha che $\sum_{j=1}^{m} y_{ji} b_j = 0 \ \forall i$. Analogamente, essendo gli elementi b_j indipendenti su F, concludiamo che $y_{ji} = 0 \ \forall (i,j)$ provando così l'indipendenza del sistema $\{b_j a_i\}_{i,j}$. $\square$

Dati Ω/F estensione di campi e $\alpha \in \Omega$, definiamo la mappa di valutazione:

$$\begin{aligned} E_\alpha : F[x] &\to \Omega \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

Osserviamo che $Im(E_\alpha) = F[\alpha]$ è il minimo sottoanello di Ω contenente sia F che α. Studiamo il nucleo $ker(E_\alpha)$:

(a) Se $ker(E_\alpha) = \{0\}$ diciamo che α è *trascendente* su F.
In tal caso E_α è iniettiva e l'immagine $F[\alpha]$ di E_α è isomorfa a $F[x]$, dominio a ideali principali che ha dimensione infinita su F.

(b) Se $ker(E_\alpha) \neq \{0\}$ diciamo che α è *algebrico* su F.
In questo caso il nucleo è l'ideale principale di $F[x]$ costituito da tutti i polinomi che si annullano in α. Vi è un unico generatore $m(x) \in F[x]$ monico. Per il Teorema di Omomorfismo $F[x]/\langle m(x) \rangle \cong Im(E_\alpha) = F[\alpha] \subseteq \Omega$ e ne segue, essendo $F[\alpha]$ un dominio, che $m(x)$ è primo e quindi irriducibile su F. Abbiamo così trovato che $F[x]/\langle m(x) \rangle$, e quindi $F[\alpha]$, è un campo. Quest'ultimo, contenendo α ed essendo contenuto in $F(\alpha)$, minimo sottocampo di Ω contenente F e α, deve coincidere con esso.
Chiamiamo $m(x)$ il *polinomio minimo di* α e definiamo $F(\alpha)$ *estensione algebrica semplice*. La dimensione $[F(\alpha) : F] = n = deg(m(x))$ ed una base di $F(\alpha)$ su F è data da $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Definizione 1.1.4. (Estensione algebrica). Un'estensione Ω/F si dice *algebrica* se ogni elemento di Ω è algebrico su F; si dice *finitamente generata* se $\exists U \subseteq \Omega$ finito tale che $\Omega = F(U)$.

Teorema 1.1.5. Sia Ω/F un'estensione di campi, sono equivalenti:

1. $[\Omega : F] < \infty$
2. Ω/F è algebrico e $[\Omega : F] < \infty$
3. $\Omega = F(\alpha_1, \ldots, \alpha_n) \quad \exists \alpha_1, \ldots, \alpha_n \in \Omega$ algebrici su F, cioè Ω/F è finitamente generata ed algebrica.

Dimostrazione. 1) $\implies$ 2) $\forall \alpha \in \Omega \quad [F(\alpha) : F]$ divide $[\Omega : F]$ per la formula dei gradi. Segue che $[F(\alpha) : F] < \infty$, ovvero α è algebrico su F. Concludiamo che Ω/F è algebrica.
2) $\implies$ 3) Essendo $[\Omega : F] < \infty$ possiamo trovare una base $\{\alpha_1, \ldots, \alpha_n\}$, si ha quindi $\Omega = F(\alpha_1, \ldots, \alpha_n)$.
3) $\implies$ 1) $[\Omega : F] = [F(\alpha_1, \ldots, \alpha_n) : F] =$
$[F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \cdot \ldots \cdot [F(\alpha_1) : F]$. Essendo tutti gli α_i algebrici ogni fattore è un intero positivo, ovvero $[\Omega : F] < \infty$. $\square$

Corollario 1.1.6. Sia Ω/F un'estensione di campi: se $A \subseteq \Omega$ è tale per cui ogni suo elemento è algebrico su F, allora $F(A)/F$ è algebrica.

Corollario 1.1.7. Siano $F \subseteq \Omega \subseteq M$ tali che Ω/F e M/Ω sono estensioni algebriche di campi. Allora M/F è algebrica.

Definizione 1.1.8. (Campo di spezzamento). Sia $f \in F[x]$ e sia Ω/F un'estensione di campi. Diremo che "f *spezza in* Ω" se è possibile scrivere

$$f(x) = a \prod_{i=1}^{n} (x - \alpha_i) \in \Omega[x], \quad \text{cioè con} \quad a, \alpha_1, \ldots, \alpha_n \in \Omega$$

Se inoltre $\Omega = F(\alpha_1, \ldots, \alpha_n)$ diremo che Ω è *campo di spezzamento* per f.

Definizione 1.1.9. (Campo algebricamente chiuso). Un campo Ω si dice *algebricamente chiuso* se ogni polinomio di grado positivo $f \in \Omega[x]$ spezza in $\Omega[x]$.

Definizione 1.1.10. (Chiusura algebrica). Un'estensione di campi Ω/F si dice *chiusura algebrica* (o che Ω è chiusura algebrica di F) se:

1. Ω/F è estensione algebrica

2. Ω è algebricamente chiuso

Teorema 1.1.11. Sia F un campo. Allora esiste una chiusura algebrica Ω/F. Se Ω_1 e Ω_2 sono tali allora esiste un F-isomorfismo $\phi : \Omega_1 \simeq \Omega_2$.

Definizione 1.1.12. (Elementi ed estensioni separabili). Sia Ω/F un'estensione algebrica.

- Diremo che $\alpha \in \Omega$ è un *elemento separabile* su F se il suo polinomio minimo $f_\alpha \in F[x]$ è separabile (cioè se le sue radici, in una qualsivoglia estensione Ω/F in cui spezzi, sono tutte semplici).

- Diremo che Ω/F è un'*estensione separabile* se ogni $\alpha \in \Omega$ è separabile su F.

Teorema 1.1.13. Sia $E = F[\alpha_1, \ldots, \alpha_r]$ un'estensione finita di F e si assuma che $\alpha_2, \ldots, \alpha_r$ siano separabili su F (non necessariamente α_1). Allora esiste un elemento $\gamma \in E$ tale che $E = F[\gamma]$.

Capitolo 2

Estensioni trascendenti

Lo scopo di questo capitolo è lo studio delle basi di trascendenza e la dimostrazione di un risultato molto importante: il teorema di Lüroth. Inizieremo con l'introdurre il concetto di indipendenza algebrica, studiandone poi alcune proprietà.

2.1 Indipendenza algebrica

Consideriamo un'estensione di campi Ω/F. Gli elementi $\alpha_1, \ldots, \alpha_n \in \Omega$ definiscono un F-omomorfismo:

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

Se il nucleo di questo omomorfismo è nullo diciamo che gli elementi α_i sono *algebricamente indipendenti* su F; in caso contrario diciamo che sono *algebricamente dipendenti*. Dunque, gli α_i sono algebricamente dipendenti su F se esiste un polinomio $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ non nullo tale per cui $f(\alpha_1, \ldots, \alpha_n) = 0$, e sono algebricamente indipendenti se:

$$\text{per ogni} \quad a_{i_1,\ldots,i_n} \in F \quad \sum a_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0 \Longrightarrow a_{i_1,\ldots,i_n} = 0 \quad \forall i_1, \ldots, i_n$$

Notiamo la similarità con l'indipendenza lineare. Infatti, se f fosse un polinomio omogeneo di grado 1, allora avremmo la definizione di indipendenza lineare.

Osservazione 2.1.1. Sia $\alpha \in \Omega$. Osserviamo che $\{\alpha\}$ è algebricamente dipendente su F se e solo se $\{\alpha\}$ è algebrico su F. Equivalentemente $\{\alpha\}$ è algebricamente indipendente su F se e solo se $\{\alpha\}$ è trascendente su F.

Diciamo che un insieme infinito A è algebricamente indipendente su F se ogni sottoinsieme finito di A è algebricamente indipendente; in caso contrario diciamo che A è algebricamente dipendente su F.
Vediamo alcuni primi esempi.

Esempio 2.1.2.

1. Per convenzione l'insieme vuoto $\emptyset$ è algebricamente indipendente.
2. I singoli $\{e\}$ e $\{\pi\}$ sono algebricamente indipendenti su $\mathbb{Q}$, ma non è ancora noto se l'insieme $\{e, \pi\}$ sia algebricamente indipendente su $\mathbb{Q}$ o meno (approfondiremo la questione nel quarto capitolo).
3. L'insieme $\{e, e^2\}$ non è algebricamente indipendente su $\mathbb{Q}$ in quanto esiste un polinomio $f(x_1, x_2) := x_1^2 - x_2$ per cui risulta $f(e, e^2) = 0$.

Sia Ω/F un'estensione di campi e sia $B = \{\alpha_1, \ldots, \alpha_n\} \subseteq \Omega$ un insieme algebricamente indipendente su F.
Allora la mappa

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

è iniettiva, dunque è un isomorfismo. Tale isomorfismo può essere esteso ai corrispondenti campi dei quozienti,

$$x_i \mapsto \alpha_i : F(x_1, \ldots, x_n) \to F(\alpha_1, \ldots, \alpha_n)$$

In questo caso, chiamiamo $F(\alpha_1, \ldots, \alpha_n)$ *estensione puramente trascendente* di F. Se $n = 1$ l'estensione si dice *semplice*.
Si può dimostrare che il polinomio

$$f(x) = x^n - \alpha_1 x^{n-1} + \cdots + (-1)^n \alpha_n \quad \in F(\alpha_1, \ldots, \alpha_n)[x]$$

ha come gruppo di Galois associato il gruppo delle permutazioni S_n (vedi [1, Teorema 5.40])

Esempio 2.1.3. $\mathbb{Q}(\pi)/\mathbb{Q}$ è un esempio di estensione puramente trascendente in quanto $\{\pi\}$ è algebricamente indipendente su $\mathbb{Q}$.

Lemma 2.1.4. Siano $\gamma \in \Omega$ e $A \subseteq \Omega$. Le seguenti affermazioni sono tra loro equivalenti:

(a) γ è algebrico su $F(A)$

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

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

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

Dimostrazione. $(a) \iff (b) \iff (c)$ sono ben noti.
$(d) \implies (c)$: scriviamo $f(x_1, ..., x_m, y)$ come un polinomio in y a coefficienti nell'anello $F[x_1, ..., x_m]$,

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

Ne segue che (c) è verificata ponendo $\beta_i = f_i(\alpha_1, ..., \alpha_m)$.
$(c) \implies (d)$: ciascun β_i in (c) per ipotesi è espressione polinomiale in un numero finito di elementi $\alpha_1, ..., \alpha_m$ di A, cioè $\beta_i = f_i(\alpha_1, ..., \alpha_m)$ con $f_i \in F[x_1, ..., x_m]$. Quindi vale (d) con $f = \sum f_i(x_1, ..., x_m)y^{n-i}$

□

Definizione 2.1.5. (Elemento algebricamente dipendente). Quando γ soddisfa le condizioni del Lemma (2.1.4), allora si dice che esso è *algebricamente dipendente* su A (sopra F). Un insieme B si dice *algebricamente dipendente* su A se ogni elemento di B è algebricamente dipendente su A.

È opportuno evidenziare le corrispondenze che si sviluppano tra l'algebra lineare e la trascendenza:

Algebra lineare	Trascendenza
indipendenza lineare	indipendenza algebrica
$A \subseteq \text{span}(B)$	A algebricamente dipendente su B
basi di spazio vettoriale	basi di trascendenza
dimensione di spazio vettoriale	grado di trascendenza

Osservazione 2.1.6. Elementi linearmente indipendenti possono essere algebricamente dipendenti. Ad esempio $\sqrt{2}$ e $\sqrt{3}$ sono linearmente indipendenti su $\mathbb{Q}$, in quanto $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (altrimenti si avrebbe $\sqrt{3} = a + b\sqrt{2}$ e, elevando al quadrato, otterremo che $\sqrt{2}$ è razionale). Tuttavia, considerando $f(x_1, x_2) = 3x_1^2 - 2x_2^2$, si ha $f(\sqrt{2}, \sqrt{3}) = 0$. Dunque $\sqrt{2}$ e $\sqrt{3}$ sono algebricamente dipendenti su $\mathbb{Q}$.

Vediamo ora un criterio che permette di verificare se un insieme è algebricamente indipendente.

Lemma 2.1.7. Sia Ω un'estensione di un campo F, siano $\alpha_1, \ldots, \alpha_n \in \Omega$. Allora sono equivalenti:

(a) L'insieme $\{\alpha_1, \ldots, \alpha_n\}$ è algebricamente indipendente su F

(b) Per ogni i, α_i è trascendente su $F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$

(c) Per ogni i, α_i è trascendente su $F(\alpha_1, \ldots, \alpha_{i-1})$

Dimostrazione. $(a) \implies (b)$ Supponiamo per assurdo che $\exists a_0, a_1, \ldots, a_{m-1} \in F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$ tali che

$$a_0 + a_1\alpha_i + \cdots + \alpha_i^m = 0 \tag{2.1}$$

Possiamo scrivere $\forall j \ a_j \in F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$ come rapporto di due funzioni polinomiali. Ponendo come minimo comune multiplo dei denominatori $b_m \in F[\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n]$ e moltiplicando (2.1) per esso otteniamo

$$b_0 + b_1\alpha_i + \cdots + b_m\alpha_i^m = 0$$

dove $b_j = g_j(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$.
Si ha che

$$f = \sum_j g_j(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)x_i^j$$

è un polinomio e $f(\alpha_1, \ldots, \alpha_n) = 0$. Questo contraddice l'ipotesi essendo che $\{\alpha_1, ..., \alpha_n\}$ sia algebricamente indipendente su F. Quindi α_i è trascendente su $F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$.
$(b) \implies (c)$ Se α_i è trascendente su $F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$, chiaramente è trascendente su un campo più piccolo $F(\alpha_1, \ldots, \alpha_{i-1})$.
$(c) \implies (a)$ Supponiamo che gli α_i non siano algebricamente indipendenti su F. Scelgo il più piccolo m tale che esiste un polinomio
$f(x_1, \ldots, x_m) \in F[x_1, ..., x_m]$ a coefficienti non nulli per il quale
$f(\alpha_1, ..., \alpha_m) = 0$. Scrivendo $f(x_1, \ldots, x_m) = \sum_j g_j x_m^j$ con $g_j \in F[x_1, ..., x_{m-1}]$, poniamo $a_j = g_j(\alpha_1, ..., \alpha_{m-1})$. Dunque

$$a_0 + a_1\alpha_m + \cdots + a_r\alpha_m^r = 0$$

Se gli a_j non sono tutti uguali a zero, allora α_m è algebrico su $F(\alpha_1, ..., \alpha_{m-1})$ e si giunge ad una contraddizione. Quindi $a_j = 0$ per ogni j. Dalla minimalità di m, si ha che $\alpha_1, ..., \alpha_{m-1}$ sono algebricamente indipendenti su F, da cui segue che $\forall j \ g_j(x_1, \ldots, x_{m-1}) = 0$ e quindi $f(x_1, \ldots, x_m) = 0$. Questo dimostra che $\alpha_1, \ldots, \alpha_n$ è algebricamente indipendente su F. $\square$

Diamo ora un risultato fondamentale che correla la cardinalità degli insiemi indipendenti con quella degli insiemi dipendenti.

Teorema 2.1.8. Sia Ω/F un'estensione di campi. Siano A=$\{\alpha_1, \ldots, \alpha_m\}$ e B=$\{\beta_1, , \ldots, \beta_n\}$ sottoinsiemi di Ω. Assumiamo:

(a) A è algebricamente indipendente (sopra F)

(b) A è algebricamente dipendente su B (sopra F)

Allora $m \leq n$.

Per dimostrarlo sfruttiamo i seguenti lemmi.

Lemma 2.1.9. (Lemma di scambio) Data l'estensione Ω/F, siano $\{\alpha_1, ..., \alpha_m\} \subseteq \Omega$ e $\beta \in \Omega$. Se β è algebricamente dipendente su $\{\alpha_1, \ldots, \alpha_m\}$, ma non su $\{\alpha_1, \ldots, \alpha_{m-1}\}$, allora α_m è algebricamente dipendente su $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$.

Dimostrazione. Poiché β è algebricamente dipendente su $\{\alpha_1, ..., \alpha_m\}$, allora esiste un polinomio $f(x_1, \ldots, x_m, y)$ a coefficienti in F tale che

$$f(\alpha_1, \ldots, \alpha_m, y) \neq 0, \quad f(\alpha_1, \ldots, \alpha_m, \beta) = 0$$

Scriviamo f come polinomio in x_m,

$$f(x_1, ..., x_m, y) = \sum_i a_i(x_1, ..., x_{m-1}, y) x_m^{n-i},$$

e osserviamo che, dato che $f(\alpha_1, \ldots, \alpha_m, y) \neq 0$, almeno uno dei polinomi

$$a_i(\alpha_1, \ldots, \alpha_{m-1}, y),$$

prendiamo a_{i_0}, è diverso dal polinomio nullo. Poiché β, per ipotesi, non è algebricamente dipendente su

$$\{\alpha_1, \ldots, \alpha_{m-1}\},$$

abbiamo che $a_{i_0}(\alpha_1, \ldots, \alpha_{m-1}, \beta) \neq 0$.
Ne consegue che $f(\alpha_1, \ldots, \alpha_{m-1}, x_m, \beta) \neq 0$. Essendo $f(\alpha_1, \ldots, \alpha_m, \beta) = 0$, questo dimostra che α_m è algebricamente dipendente su $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$. $\square$

Lemma 2.1.10. (Transitività della dipendenza algebrica) Data l'estensione Ω/F , siano A, B e C sottoinsiemi di Ω. Se C è algebricamente dipendente su B, e B è algebricamente dipendente su A, allora C è algebricamente dipendente su A.

Dimostrazione. Siano E ed F campi, dove E è un'estensione algebrica di F. Dato $\gamma \in \Omega$, se γ è algebrico su E, per come abbiamo assunto E/F, allora γ è algebrico su F. Si applichi questo ragionamento ponendo $E = F(A \cup B)$ e $F = F(A)$. □

Dimostrazione. (Teorema 2.1.8) Supponiamo che A e B abbiano k elementi in comune. Se $k = m$, allora $A \subseteq B$, e certamente $m \leq n$. Se $k < m$, consideriamo $B = \{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$. Poiché per ipotesi α_{k+1} è algebricamente dipendente su B, ma non su $\{\alpha_1, \ldots, \alpha_k\}$, esiste β_j, con $k + 1 \leq j \leq n$, tale che, a meno di riordinamento, α_{k+1} è algebricamente dipendente su $\{\alpha_1, ..., \alpha_k, \beta_{k+1}..., \beta_j\}$, ma non su $\{\alpha_1, ..., \alpha_k, \beta_{k+1}, ..., \beta_{j-1}\}$. Il lemma di scambio ci assicura che β_j è algebricamente dipendente su

$$B_1 \stackrel{def}{=} B \cup \{\alpha_{k+1}\} \setminus \{\beta_j\}$$

Quindi B è algebricamente dipendente su B_1. Per il Lemma (2.1.10), poiché A è algebricamente dipendente su B e B è algebricamente dipendente su B_1, A è algebricamente dipendente su B_1.
Se $k + 1 < m$, si ripete il ragionamento con A e B_1. Otterremo così $k = m$ e $m \leq n$.

□

2.2 Basi di trascendenza

Introduciamo ora un concetto molto simile a quello di base di uno spazio vettoriale: le basi di trascendenza.

Definizione 2.2.1. (Base di trascendenza di Ω su F). Sia Ω/F un'estensione di campi. Un sottoinsieme A di Ω si dice *base di trascendenza* di Ω su F se:

1. A è algebricamente indipendente su F
2. Ω è algebrico su F(A)

Dimostreremo ora che una base di trascendenza è caratterizzata in termini di "minimalità" in relazione alla proprietà (2) e di "massimalità" in relazione alla proprietà (1).

Proposizione 2.2.2. Siano Ω/F un'estensione di campi e $A \subseteq \Omega$. Se Ω è algebrico su $F(A)$ e A è un elemento minimale tra i sottoinsiemi di Ω rispetto a tale proprietà, allora A è una base di trascendenza di Ω su F.

Dimostrazione. Se A non è algebricamente indipendente, allora esiste un elemento $\alpha \in A$ che è algebricamente dipendente su $A \setminus \{\alpha\}$. Segue dal Lemma (2.1.10) che Ω è algebrico su $F(A \setminus \{\alpha\})$. □

Teorema 2.2.3. Sia Ω/F un'estensione di campi. Se esiste un insieme finito $A \subseteq \Omega$ tale che Ω è algebrico su $F(A)$, allora Ω ha una base di trascendenza finita su F. Inoltre, ogni base di trascendenza è finita e hanno tutte lo stesso numero di elementi.

Dimostrazione. Ogni insieme minimale $A' \subseteq A$ tale che Ω sia algebrico su $F(A')$ è una base di trascendenza. La seconda affermazione segue dal Teorema (2.1.8). □

Lemma 2.2.4. Siano Ω/F un'estensione di campi, $A \subseteq \Omega$ e $\beta \in \Omega \setminus A$. Supponiamo che A sia un insieme algebricamente indipendente e che $A \cup \{\beta\}$ sia algebricamente dipendente. Allora β è algebrico su $F(A)$.

Dimostrazione. Per ipotesi esiste un polinomio non nullo

$$f(x_1, \ldots, x_n, y) \in F[x_1, \ldots, x_n, y]$$

tale che $f(\alpha_1, \ldots, \alpha_n, \beta) = 0$, dove $\alpha_1, \ldots, \alpha_n \in A$ sono elementi distinti. Poiché A è un insieme algebricamente indipendente possiamo scrivere:

$$f = g_0 y^m + g_1 y^{m-1} + \cdots + g_m, \quad g_i \in F[x_1, \ldots, x_n], \quad g_0 \neq 0, \quad m \geq 1$$

Essendo $g_0 \neq 0$ e gli α_i algebricamente indipendenti, otteniamo che $g_0(\alpha_1, \ldots, \alpha_n) \neq 0$.
Dato che β è una radice di

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

ne consegue che è algebrico su $F(\alpha_1, \ldots, \alpha_n) \subset F(A)$. □

Proposizione 2.2.5. Data un'estensione di campi Ω/F, ogni insieme massimale tra i sottoinsiemi algebricamente indipendenti di Ω è una base di trascendenza di Ω su F.

Dimostrazione. Dobbiamo dimostrare che dato un insieme $A \subseteq \Omega$ algebricamente indipendente massimale abbiamo che Ω è algebrico su $F(A)$. Dalla massimalità di A segue che $\forall \beta \in \Omega \setminus A$, $A \cup \{\beta\}$ è algebricamente dipendente. Dunque, sfruttando il lemma precedente, abbiamo che β è algebrico su $F(A)$. Concludiamo che Ω è algebrico su $F(A)$. □

Teorema 2.2.6. Sia Ω/F un'estensione di campi. Ogni sottoinsieme S algebricamente indipendente di Ω, è contenuto in una base di trascendenza di Ω su F. In particolare, ogni estensione ammette una base di trascendenza.

Dimostrazione. Sia $\mathcal{M}$ l'insieme dei sottoinsiemi algebricamente indipendenti di Ω contenenti S. Notiamo che $\mathcal{M}$ è parzialmente ordinato per inclusione. Sia T un sottoinsieme totalmente ordinato di $\mathcal{M}$, e sia $B = \bigcup\{A|A \in T\}$. Vogliamo dimostrare che $B \in \mathcal{M}$, cioè che B è algebricamente indipendente. Se così non fosse, esisterebbe un sottoinsieme finito di B, che chiamiamo B', che non è algebricamente indipendente. Tuttavia, in tal caso B' sarebbe contenuto in un elemento di T, si arriva così ad una contraddizione. Il Lemma di Zorn ci assicura che $\mathcal{M}$ ammette un elemento massimale, cioè esiste un insieme indipendente massimale contenente S. La Proposizione (2.2.5) dimostra che tale insieme è una base di trascendenza di Ω su F. □

Esempio 2.2.7.

1. Sia Ω/F è un'estensione di campi, allora $\emptyset$ è una base di trascendenza per Ω/F se e solo se Ω/F è algebrica.

2. Sia Ω/F un'estensione di campi. Se $\Omega = F(x_1, \ldots, x_n)$ allora l'insieme di indeterminate $\{x_1, \ldots, x_n\}$ è una base di trascendenza di Ω su F. Inoltre, presi $r_1, \ldots, r_n$ interi positivi, si ha che $\{x_1^{r_1}, \ldots, x_n^{r_n}\}$ è una base di trascendenza per Ω/F. Dobbiamo dimostrare l'indipendenza algebrica di $\{x_1^{r_1}, \ldots, x_n^{r_n}\}$ e l'algebricità di Ω su $F(x_1^{r_1}, \ldots, x_n^{r_n})$.
   Studiamo il caso base: $\{x_1, \ldots, x_n\}$.
   Sappiamo che $F(x_1, \ldots, x_n)$ è il minimo campo che contiene sia F che $\{x_1, \ldots, x_n\}$. Se l'insieme di indeterminate fosse algebricamente dipendente avremmo che $\exists i$ t.c. x_i può essere espressa come combinazione delle altre.
   Avremmo trovato che $F(x_1, .., x_{i-1}, x_{i+1}, ..x_n) = F(x_1, \ldots, x_n)$, che è assurdo. Per provare l'indipendenza algebrica di $\{x_1^{r_1}, \ldots, x_n^{r_n}\}$ procediamo in modo analogo. Se le potenze fossero algebricamente dipendenti allora $\exists f(x_1^{r_1}, \ldots, x_n^{r_n}) = 0$ con $f(y_1, \ldots, y_n) \neq 0 \in F[y_1, \ldots, y_n]$ in contraddizione con l'ipotesi iniziale. Per verificare che Ω è algebrico su $F(x_1^{r_1}, \ldots, x_n^{r_n})$ basta osservare che ciascun x_i è zero del polinomio $t_i^{r_i} - x_i^{r_i} \in F(x_1^{r_1}, \ldots, x_n^{r_n})[t]$.

2.3 Grado di trascendenza

È possibile dimostrare che il Teorema (2.2.3) si estende anche al caso infinito: la cardinalità di ogni base di trascendenza è invariante. Ciò rende possibile la seguente.

Definizione 2.3.1. (Grado di trascendenza di Ω su F). Data Ω/F estensione di campi, il *grado di trascendenza di* Ω *su* F è la cardinalità di una (qualsiasi) base di trascendenza di Ω su F. Essa si denota con $trdeg_F\Omega$.

Per esempio, l'estensione puramente trascendente $F(x_1, \ldots, x_n)$ di F ha grado di trascendenza n.

Useremo il simbolo $|B|$ per indicare la cardinalità di un insieme B.

Osservazione 2.3.2. Ci sono tre possibilità:

- Ω è algebrico su F: il suo grado di trascendenza è uguale a zero;
- Ω ha una base di trascendenza finita su F: il suo grado di trascendenza è uguale al massimo numero di elementi di Ω algebricamente indipendenti su F;
- Ω ha una base di trascendenza infinita su F: il suo grado di trascendenza è infinito.

Proposizione 2.3.3. Siano L e M campi algebricamente chiusi e con lo stesso grado di trascendenza su un campo F. Allora sono F-isomorfi.

Dimostrazione. Siano A e A' basi di trascendenza dei campi L e M, rispettivamente. Per ipotesi esiste una biezione $A \to A'$, che definisce un F-isomorfismo $F[A] \to F[A']$ che si estende ad un isomorfismo $F(A) \to F(A')$ definito tra i corrispondenti campi dei quozienti. Attraverso tale isomorfismo si identificano $F(A)$ e $F(A')$. Essendo i campi di partenza, L e M, chiusure algebriche di campi isomorfi, $F(A)$ e $F(A')$, segue dal Teorema (1.1.11) che sono F-isomorfi. $\square$

Osservazione 2.3.4. Due campi algebricamente chiusi con la stessa cardinalità non numerabile e la stessa caratteristica sono isomorfi. L'idea alla base della dimostrazione è la seguente. Siano F e F' i sottocampi fondamentali, cioè i più piccoli sottocampi di Ω e Ω'; possiamo identificare F con F'. A questo punto si dimostra che quando Ω non è numerabile, la cardinalità di Ω coincide con quella di una base di trascendenza su F. Si applica la Proposizione (2.3.3) per concludere.

Consideriamo ora due estensioni di campi M/Ω e Ω/F. I teoremi che seguono ci permetteranno di comparare i gradi di trascendenza in questo caso.

Teorema 2.3.5. Dati M/Ω e Ω/F estensioni di campi, A un sottoinsieme di Ω algebricamente indipendente su F e B un sottoinsieme di M algebricamente indipendente su Ω, allora $A \cup B$ è algebricamente indipendente su F.

Dimostrazione. Sia C un sottoinsieme finito di $A \cup B$. Possiamo scrivere

$$C = \{\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s\}$$

tale che $\alpha_i \in A, \beta_j \in B$.
Per il Lemma (2.1.7) α_i è trascendente su $F(\alpha_1, \dots, \alpha_{i-1})$ per $1 \leq i \leq r$ e β_j è trascendente su $\Omega(\beta_1, \dots, \beta_{j-1})$ per $1 \leq j \leq s$. Quindi β_j è trascendente su $F(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_{j-1})$ per $1 \leq j \leq s$. Utilizzando nuovamente il Lemma (2.1.7), abbiamo che C è algebricamente indipendente su F. Poiché quanto abbiamo appena dimostrato vale per un qualsiasi sottoinsieme finito di $A \cup B$, $A \cup B$ è algebricamente indipendente su F. □

Teorema 2.3.6. Dati M/Ω e Ω/F estensioni di campi, A una base di trascendenza di Ω su F e B una base di trascendenza di M su Ω, allora $A \cup B$ è una base di trascendenza di M su F.

Dimostrazione. Usufruiamo del teorema precedente e della definizione di base di trascendenza: sappiamo che $A \cup B$ è algebricamente indipendente su F, quindi rimane da dimostrare che M è algebrica su $F(A \cup B)$. Poiché A è una base di trascendenza di Ω su F, $\Omega/F(A)$ è algebrica.
Dato che $F(A) \subseteq F(A \cup B)$, segue che anche $F(A \cup B)(\Omega)/F(A \cup B)$ è algebrica. Essendo $F(A \cup B)(\Omega) = \Omega(B)$, $\Omega(B)/F(A \cup B)$ è algebrica. Analogamente poiché B è una base di trascendenza di M su Ω, $M/\Omega(B)$ è anch'essa algebrica. Concludiamo dal Corollario (1.1.7) che $M/F(A \cup B)$ è algebrica. □

Corollario 2.3.7. Siano M/Ω e Ω/F estensioni di campi. Si ha:

$$trdeg_F M = trdeg_\Omega M + trdeg_F \Omega \tag{2.2}$$

Dimostrazione. Immediata conseguenza del teorema precedente. □

Corollario 2.3.8. Siano M/Ω e Ω/F estensioni di campi. Se M/Ω è un'estensione algebrica, una base di trascendenza di Ω/F è anche una base di trascendenza di M/F. In particolare M e Ω hanno lo stesso grado di trascendenza su F.

Dimostrazione. Consideriamo A e B definite come nel Teorema (2.3.6). Data l'algebricità di M su Ω per ipotesi, abbiamo $B = \emptyset$. Segue dal teorema appena citato che $A \cup B = A$ è base di trascendenza di M/F. Concludiamo grazie al corollario precedente. □

Esempio 2.3.9. Poiché π è trascendente su $\mathbb{Q}$, le estensioni di campi $\mathbb{Q}(\pi)/\mathbb{Q}$ e $\mathbb{Q}(\pi, \sqrt{2})/\mathbb{Q}$ hanno entrambe grado di trascendenza uguale a 1 (basta utilizzare il Corollario (2.3.7) ponendo $M = \mathbb{Q}(\pi, \sqrt{2}),\ \Omega = \mathbb{Q}(\sqrt{2}),\ F = \mathbb{Q}$).

Esempio 2.3.10. Il grado di trascendenza di $\mathbb{R}$ e di $\mathbb{C}$ su $\mathbb{Q}$ è uguale alla cardinalità del continuo. Studieremo nel dettaglio il caso di $\mathbb{R}$ quando analizzeremo il Teorema di Cantor (3.3.7) nel terzo capitolo dell'elaborato. Osserviamo che $\mathbb{C}$ ha lo stesso grado di trascendenza di $\mathbb{R}$ su $\mathbb{Q}$ perchè è algebrico su $\mathbb{R}$ (Corollario (2.3.8)).

2.3.1 I polinomi simmetrici elementari

I polinomi simmetrici elementari sono un esempio fondamentale di base di trascendenza del campo delle funzioni razionali $F(x_1, \ldots, x_n)$ su F. Definiamoli e dimostriamo quanto appena affermato.

Definizione 2.3.11. (Polinomio simmetrico). Dato un campo F e un insieme ordinato $x = \{x_1, \ldots, x_n\}$ di indeterminate su F, un polinomio $f(x_1, \ldots, x_n) \in F[x]$ si dice *polinomio simmetrico* se $f(x) = f(x_{\sigma_{(1)}}, \ldots, x_{\sigma_{(n)}})$ per ogni permutazione $\sigma \in S_n$, ovvero se $f(x)$ rimane invariato per una qualsiasi permutazione delle indeterminate $\{x_1, \ldots, x_n\}$. In particolare, si definiscono i *polinomi simmetrici elementari* nel seguente modo:

$$
\begin{aligned}
s_1 &:= \sum_{i=1,\ldots,n} x_i \ ; \\
s_2 &:= \sum_{1 \le i_1 < i_2 \le n} x_{i_1} x_{i_2} \ ; \\
&\ldots\ldots\ldots \\
s_r &:= \sum_{1 \le i_1 < \cdots < i_r \le n} x_{i_1} x_{i_2} \ldots x_{i_r} \\
&\ldots\ldots\ldots \\
s_n &:= x_1 \ldots x_n
\end{aligned}
$$

Osserviamo che i polinomi simmetrici elementari in $\{x_1, \ldots, x_{n-1}\}$, si ottengono da $s_1, \ldots, s_{n-1}$ ponendo $x_n = 0$.
Affinché essi costituiscano una base di trascendenza di $F(x_1, \ldots, x_n)$ su F devono essere verificate le seguenti condizioni:

- $\{s_1, \ldots, s_n\} \subseteq F(x_1, \ldots, x_n)$ è algebricamente indipendente su F
- $F(x_1, \ldots, x_n)$ è algebrico su $F(s_1, \ldots, s_n)$

Il seguente risultato ci permette di dimostrare il primo asserto.

Teorema 2.3.12. Sia F un dominio e sia $x := \{x_1, \dots, x_n\}$ un insieme ordinato di indeterminate su F. Allora l'applicazione

$$\begin{aligned} \psi : F(x) &\to F(x) \\ f(x_1, \dots, x_n) &\mapsto f(s_1 \dots, s_n) \end{aligned}$$

è un omomorfismo iniettivo, per ogni $n \geq 1$.

Dimostrazione. Vedi [2, Teorema 2.7.6] □

L'indipendenza algebrica di $\{s_1, \dots, s_n\}$ su F segue dall'iniettività di ψ.

Per verificare il secondo asserto dobbiamo dare prima la definizione di *polinomio generale di grado n.*

Definizione 2.3.13. (Polinomio generale di grado n). Sia F un dominio e siano $x_1, \dots, x_n, t$ indeterminate su F. Il polinomio

$$G(x,t) := (t - x_1)(t - x_2) \dots (t - x_n) \in F(x,t)$$

è detto polinomio generale di grado n su F. Sviluppando i prodotti e mettendo in evidenza le potenze di t si ottiene

$$G(x,t) := g(t) := t^n - s_1 t^{n-1} + s_2 t^{n-2} - \dots + (-1)^n s_n$$

dove $s_1, \dots, s_n$ sono i polinomi simmetrici elementari in $x_1, \dots, x_n$.
In particolare, $g(t) \in F(s_1, \dots, s_n)$ ed ha radici $x_1, \dots, x_n \in F(x)$.

Evidentemente un campo di spezzamento di $g(t)$ su $F(s_1, \dots, s_n)$ è il campo delle funzioni razionali $F(x_1, \dots, x_n)$. Segue banalmente l'algebricità di $F(x_1, \dots, x_n)$ su $F(s_1, \dots, s_n)$.

Concludiamo così che $\{s_1, \dots, s_n\}$ costituisce una base di trascendenza di $F(x_1, \dots, x_n)$ su F.

2.4 Teorema di Lüroth

Supponiamo che Ω/F sia un'estensione finitamente generata che ha grado di trascendenza r. Se $\{\alpha_1, \dots, \alpha_r\}$ è una base di trascendenza per Ω su F, allora $\Omega/F(\alpha_1, \dots, \alpha_r)$ è un'estensione algebrica finita. Se troviamo una base di trascendenza tale che $\Omega = F(\alpha_1, \dots, \alpha_r)$, allora Ω è puramente trascendente su F per definizione. Tuttavia non è sempre semplice determinare quando

un'estensione finitamente generata sia puramente trascendente o meno. Il Teorema di Lüroth ci aiuta a risolvere questo problema. Ai fini della dimostrazione richiamiamo il Lemma di Gauss e alcune sue conseguenze.

Siano R un dominio a fattorizzazione unica e Q il suo campo dei quozienti, ad esempio $R = F[x]$ e $Q = F(x)$. Un polinomio $f(t) = \sum a_i t^i \in R[t]$ si dice primitivo se i suoi coefficienti a_i non hanno alcun fattore in comune a parte un'unità. Ciascun polinomio $f \in Q[x]$ può essere scritto come $f = c(f) \cdot f_1$, dove $c(f) \in Q$ e f_1 è primitivo (scriviamo $f = af/a$ con a un denominatore comune dei coefficienti di f, e in seguito $f = (b/a)f_1$ con b il massimo comune divisore dei coefficienti di af). L'elemento $c(f)$ è univocamente determinato, e $f \in R[x]$ se e solo se $c(f) \in R$.

Proposizione 2.4.1. Se $f, g \in R[t]$ sono primitivi, allora lo è anche il prodotto $f \cdot g$.

Dimostrazione. Siano $f = \sum a_i t^i$ e $g = \sum b_i t^i$, e sia p un elemento primo di R. Poiché f è primitivo, $\exists a_i$ non divisibile per p. Sia a_{i_1} il primo di tali coefficienti. Analogamente, sia b_{i_2} il primo coefficiente di g non divisibile per p. Si ha quindi che il coefficiente di $t^{i_1+i_2}$ nel polinomio $f \cdot g$ non è divisibile per p. Ciò dimostra che $f \cdot g$ è primitivo. □

Proposizione 2.4.2. Dati $f, g \in R[t]$, si hanno $c(fg) = c(f)c(g)$ e $(fg)_1 = f_1 g_1$.

Dimostrazione. Siano $f = c(f)f_1$ e $g = c(g)g_1$ con f_1 e g_1 primitivi. Allora $fg = c(f)c(g)f_1 g_1$ con $f_1 g_1$ primitivo. Otteniamo così che $c(fg) = c(f)c(g)$ e $(fg)_1 = f_1 g_1$. □

Lemma 2.4.3. (Lemma di Gauss) Sia f un polinomio in $R[t]$. Se f si fattorizza nel prodotto di due polinomi non costanti in $Q[t]$, allora si fattorizza nel prodotto di due polinomi non costanti in $R[t]$.

Dimostrazione. Supponiamo che $f = gh \in Q[t]$. Allora $f_1 = g_1 h_1 \in R[t]$, e possiamo fattorizzare f in $R[t]$ in questo modo: $f = c(f)f_1 = (c(f)g_1)h_1$. □

Proposizione 2.4.4. Siano $f, g \in R[t]$. Se f divide g in $Q[t]$ e f è primitivo, allora f divide g in $R[t]$.

Dimostrazione. Sia $fq = g$, dove $q \in Q[t]$. Allora $c(q) = c(g) \in R$, e quindi $q \in R[t]$. □

Dimostriamo ora il Teorema di Lüroth.
Dato $u \in F(x)$ definiamo il grado $deg(u)$ come il maggiore tra i gradi del numeratore e del denominatore di u, quando u è espresso nella sua forma semplice.

Lemma 2.4.5. Sia $u \in F(x) \setminus F$. Allora u è trascendente su F, x è algebrico su $F(u)$ e $[F(x) : F(u)] = deg(u)$.

Dimostrazione. Sia $u(x) = a(x)/b(x)$ con $a(x)$ e $b(x)$ coprimi. Allora $a(t) - b(t)u$ è un polinomio in $F(u)[t]$ che ha x come radice, quindi x è algebrico su $F(u)$. Segue che u è trascendente su F (altrimenti x sarebbe algebrico su F [1, Corollario 1.31]).
Il polinomio $a(t) - b(t)z \in F[z, t]$ è chiaramente irriducibile. Poiché u è trascendente su F,

$$F[z, t] \cong F[u, t], \quad z \leftrightarrow u, \quad t \leftrightarrow t$$

allora anche $a(t) - b(t)u$ è irriducibile in $F[u, t]$, e quindi anche in $F(u)[t]$ per il Lemma di Gauss. Inoltre ha x come radice, e quindi, a meno di costanti, è il polinomio minimo di x su $F(u)$, e ha grado $deg(u)$, che conclude la dimostrazione del lemma. □

Esempio 2.4.6. Abbiamo che $F(x) = F(u)$ se e solo se

$$u = \frac{ax + b}{cx + d}$$

con $ad - bc \neq 0$.

Teorema 2.4.7. (Teorema di Lüroth) Sia $L = F(x)$ un'estensione trascendente semplice. Allora ogni sottocampo E di L che contiene propriamente F è della forma $E = F(u)$ per qualche $u \in L$ trascendente su F.

Dimostrazione. Se $u \in E \setminus F$ allora $F \subset E \subseteq F(x) = L$ e

$$[F(x) : E] \leq [F(x) : F(u)] = deg(u) < \infty$$

Quindi x è algebrico su E. Sia $f(t)$ il polinomio minimo di x su E:

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_n, \quad a_i \in E, \quad n = [F(x) : E] \tag{2.3}$$

Poiché x è trascendente su F, almeno uno dei coefficienti a_j non appartiene ad F, e mostreremo che $E = F(a_j)$ per un tale a_j.
Sia $d(x) \in F[x]$ un polinomio di grado minimo tale che $d(x)a_i(x) \in F[x]$ $\forall i$, e sia

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

Allora f_1 è primitivo come polinomio in t, cioè $MCD(d, da_1, \ldots, da_n) = 1$ in $F[x]$. Il grado m di f_1 in x è il grado massimo di uno dei polinomi $da_1,\ da_2, \ldots da_n$, cioè

$$m = deg(da_i)$$

Scriviamo $a_i = \frac{b}{c}$ con b, c coprimi in $F[x]$.
Consideriamo il polinomio $b(t) - c(t)a_i(x)$ in $E[t]$ avente x come radice.
Dunque esso è divisibile per f: $\exists q(t) \in E[t]$ t.c.

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

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

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

Dato che f_1 differisce da f per un elemento non nullo in $F(x)$, l'equazione mostra che f_1 divide $p(x,t) := c(x) \cdot b(t) - c(t) \cdot b(x)$ in $F(x)[t]$. Poiché f_1 è primitivo in $F[x][t] = F[x,t]$, per la Proposizione (2.4.4) si ha che esiste un polinomio $h \in F[x,t]$ tale che

$$f_1(x,t) \cdot h(x,t) = p(x,t). \tag{2.4}$$

Nella (2.4) il polinomio $p(x,t)$ ha grado al massimo m in x, e $f_1(x,t)$ ha grado m in x. Dunque $p(x,t)$ ha grado esattamente m in x e $h(x,t)$ ha grado 0 in x. Ma allora $h(t,x) = h(t) \in F[t]$. Dalla (2.4) segue che $p(x,t)$ non è divisibile per un polinomio non costante in $F[x]$. Inoltre $p(x,t)$ è simmetrico in x e t; quindi ha stesso grado sia rispetto a x che a t. Perciò ha grado m in t e non è divisibile per un polinomio non costante in $F[t]$: segue che $h(t)$ è una costante non nulla di F. Concludiamo che $f_1(x,t)$ è multiplo costante di $p(x,t)$. Comparando i gradi in (2.4), vediamo che m e n risultano uguali. Dunque

$$[F(x) : F(a_i)] = \deg(a_i) \leq \deg(da_i) = m = n = [F(x) : E] \leq [F(x) : F(a_i)].$$

Vale quindi l'uguaglianza, e $E = F[a_i]$.

Ora, dal fatto che $a_j \notin F$, si deduce che

$$[F(x) : E] \leq [F(x) : F(a_j)] = \deg(a_j) \leq \deg(da_i) = m = [F(x) : E]$$

e concludiamo che $E = F(a_j)$.

□

Osservazione 2.4.8. Il Teorema di Lüroth non si può estendere al caso di due o più indeterminate - si vedano gli esempi di Zariski [1, Footnote 5.5] e di Swan [1, Remark 5.41]. Ciononostante, risulta vero quanto segue: se $[F(x,y) : E] < \infty$ e F è algebricamente chiuso di caratteristica zero, allora E/F è un'estensione puramente trascendente (Teorema di Zariski, 1958).

Luröth dimostrò il suo teorema su $\mathbb{C}$ nel 1876. Per i campi generali, fu dimostrato da Steinitz nel 1910, tramite l'argomento sopra riportato.

2.5 Basi di trascendenza separanti

Sia E/F un'estensione di campi finitamente generata.
Un sottoinsieme $\{x_1, \ldots, x_d\}$ di E è una *base di trascendenza separante* per E/F se è un insieme algebricamente indipendente sopra F ed E è un'estensione finita algebrica separabile di $F(x_1, \ldots, x_d)$.

Teorema 2.5.1. Se F è un campo perfetto, allora ogni estensione finitamente generata E di F ammette una base di trascendenza separante su F.

Dimostrazione. Se F ha caratteristica zero, allora ogni base di trascendenza è separante, dunque l'enunciato si riconduce a quello del Teorema (2.2.3). Assumiamo quindi che F abbia caratteristica $p \neq 0$. Poiché F è perfetto, ogni polinomio in $x_1^p, \ldots, x_n^p$ con coefficienti in F è una potenza p-esima in $F[x_1, \ldots, x_n]$:

$$\sum a_{i_1 \ldots i_n} x_1^{i_1 p} \ldots x_n^{i_n p} = (\sum a_{i_1 \ldots i_n}^{(\frac{1}{p})} x_1^{i_1} \ldots x_n^{i_n})^p$$

Sia $E = F(x_1, \ldots, x_n)$, e assumiamo che $n > d + 1$, dove d è il grado di trascendenza di E su F. Rinumeriamo gli indici affinché $x_1, \ldots, x_n$ costituiscano un insieme algebricamente indipendente (si veda (2.2.2)). Allora esiste un polinomio irriducibile non nullo $f(x_1, \ldots, x_{d+1}) = 0$ con coefficienti in F. Le derivate parziali $\partial f / \partial x_i$ non sono tutte nulle, altrimenti si avrebbe che f sarebbe un polinomio in $x_1^p, \ldots, x_{d+1}^p$, cioè una potenza p-esima. Dopo aver rinumerato $x_1, \ldots, x_{d+1}$, supponiamo che $\partial f / \partial x_{d+1} \neq 0$. Allora abbiamo che x_{d+1} è un elemento separabile e algebrico su $F(x_1, \ldots, x_d)$, e $F(x_1, \ldots, x_{d+1}, x_{d+2})$ è algebrico su $F(x_1, \ldots, x_{d+1})$ e dunque anche su $F(x_1, \ldots, x_d)$. Per il Teorema dell'elemento primitivo (1.1.13) $\exists y$ tale che $F(x_1, \ldots, x_{d+2}) = F(x_1, \ldots, x_d, y)$.
Abbiamo così che E è generato da $n - 1$ elementi (come campo contenente F). Ripetendo tale procedimento, possibilmente più volte, otterremo che $E = F(z_1, \ldots, z_{d+1})$ con z_{d+1} separabile su $F(z_1, \ldots, z_d)$. $\square$

Capitolo 3

I numeri trascendenti

3.1 Accenni storici

Lo studio dei numeri trascendenti, diversamente da quello dei numeri algebrici, presenta molteplici aspetti che sembra non possano ricondursi ad una teoria generale. L'esistenza dei numeri trascendenti è stata dimostrata da J. Liouville nel 1844, come conseguenza del suo celebre *Teorema di Approssimazione*. Egli osservò che i numeri la cui forma decimale contiene un numero elevato di zeri sono trascendenti; uno dei *numeri di Liouville* più noto è il numero $\sum_{k\geq 1} \frac{1}{10^{k!}}$. Una dimostrazione indiretta dell'esistenza dei numeri trascendenti è stata poi data da G.F. Cantor, nel 1874. Essa si basa sul fatto che l'insieme dei numeri algebrici ha cardinalità del numerabile, mentre il campo dei numeri reali ha cardinalità strettamente maggiore; i numeri trascendenti sono quindi infinitamente più numerosi dei numeri algebrici. Tuttavia, in generale, dimostrare la trascendenza, o anche soltanto l'irrazionalità, di un particolare numero reale risulta alquanto difficile. Ad esempio, la trascendenza del numero di Nepero e fu congetturata da L. Euler nel 1784, ma venne dimostrata da C. Hermite solo nel 1873. Nove anni dopo, nel 1882, F. Lindemann generalizzò il *Teorema di Hermite* per dimostrare la trascendenza di π. Tale dimostrazione risulta rilevante perchè implica l'impossibilità di costruire con riga e compasso un quadrato che abbia area uguale a quella di un cerchio assegnato. Nel 1934 vennero effettuati ulteriori sviluppi da parte di A. Gelfond e T. Schneider i quali risolsero il settimo problema di Hilbert che chiedeva di stabilire se i numeri del tipo α^β, con α e β algebrici, fossero trascendenti. Negli ultimi anni la congettura di Schanuel (vedi Sezione (4.3)) ha giocato un ruolo fondamentale in teoria dei numeri trascendenti. Formulata agli inizi degli anni sessanta, tale congettura non è ancora stata dimostrata, ma potrebbe portare a delle conseguenze molto importanti come

l'indipendenza algebrica di $\{e, \pi\}$.

3.2 I numeri di Liouville

Lo scopo di questa sezione è la dimostrazione del Teorema di Lioviulle. Il suo asserto riguarda l'approssimazione dei numeri trascendenti e permise al matematico francese di costruire esplicitamente i primi numeri trascendenti, ovvero i *numeri di Liouville*.

Teorema 3.2.1. (J.Liouville, 1844) Sia $\alpha \in \mathbb{R}$ un numero algebrico, radice di un polinomio a coefficienti interi, di grado d. Allora esiste un numero reale positivo M, tale che per ogni coppia di interi p, q con $q > M$ vale

$$\alpha = \frac{p}{q} \quad \text{oppure} \quad \left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{d+1}} \tag{3.1}$$

Dimostrazione. Sia $h(t)$ un polinomio di grado d a coefficienti interi tale che $h(\alpha) = 0$ e sia $\delta > 0$ tale che $h(t)$ non abbia radici diverse da α nell'intervallo $[\alpha - \delta, \alpha + \delta]$. Indichiamo con m il massimo della funzione continua $|h'(t)|$ nell'intervallo appena considerato e definiamo

$$M = max(m, \sqrt[d+1]{\frac{1}{\delta}})$$

Dato $q > M$ per ipotesi, si hanno le seguenti disuguaglianze:

$$q^{d+1} > M^{d+1} \geq \frac{1}{\delta} \qquad \frac{1}{q^{d+1}} < \delta$$

Se $\alpha = \frac{p}{q}$ oppure $|\alpha - \frac{p}{q}| > \delta$ il risultato è banalmente vero.
Se $\left|\alpha - \frac{p}{q}\right| \leq \delta$ e $\alpha \neq \frac{p}{q}$, allora per il teorema del valor medio esiste $\xi \in [\alpha - \delta, \alpha + \delta]$ tale che

$$0 \neq h\left(\frac{p}{q}\right) = h\left(\frac{p}{q}\right) - h(\alpha) = h'(\xi)\left(\frac{p}{q} - \alpha\right)$$

Moltiplicando per q^d e prendendo il valore assoluto otteniamo

$$q^d h\left(\frac{p}{q}\right) = q^d |h'(\xi)| \left|\frac{p}{q} - \alpha\right| \leq q^d m \left|\frac{p}{q} - \alpha\right|$$

Sapendo che $q^d h(\frac{p}{q})$ è un intero non nullo, il suo valore assoluto è ≥ 1. Abbiamo così

$$1 \leq \left|q^d h\left(\frac{p}{q}\right)\right| \leq q^d m \left|\frac{p}{q} - \alpha\right|$$

da cui deduciamo

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{q^d m} \geq \frac{1}{q^d M} \geq \frac{1}{q^{d+1}}$$

□

Corollario 3.2.2. Il numero di Liouville $\sum_n \frac{1}{10^{n!}}$ è trascendente.

Dimostrazione. Sia $N > 0$, scriviamo

$$l = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = \frac{p}{10^{N!}} + \sum_{n=N+1}^{\infty} \frac{1}{10^{n!}}$$

per un opportuno numero intero p. Si verifica facilmente che:

$$\left|l - \frac{p}{10^{N!}}\right| = \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!}} = \frac{1}{10^{(N!)N}} \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!-(N!)N}} < \frac{1}{10^{(N!)N}}$$

Se l fosse algebrico di grado d, per $N > d$ e sufficientemente grande otterremmo una stima che contraddice il Teorema (3.2.1). □

3.3 L'esistenza dei numeri trascendenti

In questa sezione richiamiamo alcune nozioni riguardanti la teoria degli insiemi, necessarie a dimostrare l'esistenza dei numeri trascendenti.

La cardinalità dell'insieme $\mathbb{N}$ dei numeri naturali si chiama *cardinalità del numerabile* e si dice che X è un insieme numerabile se $|X| = |\mathbb{N}|$. Ricordiamo che $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili. Al contrario, il campo reale $\mathbb{R}$ non è numerabile e la cardinalità di $\mathbb{R}$ si chiama *cardinalità del continuo*. Segue dal *"Secondo procedimento diagonale di Cantor"* (vedi [2, Teorema 13.2.2]) che la cardinalità del continuo è strettamente maggiore della cardinalità del numerabile, e che $|\mathbb{R}| = |P(\mathbb{N})|$.

Le dimostrazioni dei seguenti risultati si possono trovare in [2, Sezione 13.1].

Teorema 3.3.1. L'unione di una famiglia numerabile di insiemi numerabili è un insieme numerabile.

Proposizione 3.3.2. Se X è un insieme finito o numerabile e Y è infinito, allora $|X \cup Y| = |Y|$.

Proposizione 3.3.3. Se X è un insieme finito o numerabile e Y è numerabile, il prodotto diretto $X \times Y$ è numerabile.

Dimostriamo ora che l'anello dei polinomi $\mathbb{Q}[x]$ è numerabile. Sfrutteremo tale asserto per provare che l'insieme di tutti i numeri algebrici è numerabile.

Corollario 3.3.4. Se A è un dominio numerabile, l'anello $A[x]$ dei polinomi in una variabile a coefficienti in A è numerabile. In particolare gli anelli $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ sono numerabili.

Dimostrazione. Per ogni $d \geq 0$, indichiamo con P_d l'insieme dei polinomi di grado d. Per il principio di identità dei polinomi, la corrispondenza che associa ad ogni polinomio di grado d la $(d+1)$-pla dei suoi coefficienti è una corrispondenza biunivoca tra P_d e il prodotto diretto di $d+1$ copie di A. Quindi, poiché A è numerabile, anche P_d è numerabile (Proposizione (3.3.3)). Per finire, notiamo che $A[x] = \left(\bigcup_{d\geq 0} P_d\right) \cup \{0\}$. Quindi $A[x]$ è numerabile per il Teorema (3.3.1).
La numerabilità di $\mathbb{Z}[x]$ e di $\mathbb{Q}[x]$ segue dal fatto che $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili. □

Osservazione 3.3.5. Per induzione su $n \geq 1$ dal Corollario (3.3.4) si ottiene che, se A è numerabile, anche l'anello dei polinomi in n variabili su A è numerabile.

Corollario 3.3.6. L'insieme $\mathcal{A}$ di tutti i numeri algebrici è numerabile.

Dimostrazione. Ogni numero algebrico è radice di un polinomio non nullo a coefficienti razionali ed ogni polinomio $f(x)$ di grado $n \geq 1$ ha al più n radici distinte. Indicando con R_f l'insieme delle radici di $f(x)$ risulta allora

$$\mathcal{A} = \bigcup \{R_f;\, f(x) \in \mathbb{Q}[x], f(x) \neq 0\}$$

Poiché $\mathbb{Q}[x]$ è numerabile (Corollario (3.3.4)), $\mathcal{A}$ è numerabile per il Teorema (3.3.1). □

Siamo giunti alla dimostrazione principale della sezione che utilizza quanto attestano i risultati appena provati.

Teorema 3.3.7. (G. Cantor, 1874) L'insieme dei numeri reali trascendenti ha la cardinalità del continuo.

Dimostrazione. Applichiamo la Proposizione (3.3.2) all'insieme dei numeri reali scrivendo $\mathbb{R} = (\mathbb{R} \setminus \mathcal{A}) \cup (\mathcal{A})$.
Posti $X = \mathbb{R} \setminus \mathcal{A}$ e $Y = \mathcal{A}$, supponiamo per assurdo che X sia finito o numerabile. Allora abbiamo che $|\mathbb{R}| = |\mathbb{R} \setminus \mathcal{A}| \cup |\mathcal{A}| = |\mathcal{A}|$. Sappiamo che l'insieme $\mathcal{A}$ di tutti i numeri algebrici è numerabile (Corollario (3.3.6)) e il campo reale $\mathbb{R}$ ha cardinalità strettamente maggiore.
Si arriva ad una contraddizione. □

Capitolo 4

La trascendenza di e e π

In questo capitolo trattiamo due esempi rilevanti di numeri trascendenti: e e π. Inizieremo con l'introdurre due teoremi: il teorema di C. Hermite e il teorema di F. Lindemann. Successivamente esploreremo le conseguenze e i risultati fondamentali a cui essi hanno portato, tra cui la trascendenza di e e π.

Teorema 4.0.1. (C. Hermite, 1873) Se $\alpha_1, \ldots, \alpha_n$ sono numeri razionali distinti, $n \geq 1$, i numeri $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sono linearmente indipendenti su $\mathbb{Q}$.

Il Teorema di Hermite è stato generalizzato da F. Lindemann nel 1882.

Teorema 4.0.2. (F. Lindemann, 1882) Scelti comunque n numeri algebrici distinti α_i e n numeri algebrici non nulli A_i, $1 \leq i \leq n$ risulta

$$A_1 e^{\alpha_1} + A_2 e^{\alpha_2} + \cdots + A_n e^{\alpha_n} \neq 0$$

Tale asserto venne dimostrato in maniera rigorosa da Weierstrass nel 1885. Una dimostrazione del Teorema di Lindemann si può trovare in [6, Teorema 1.4].

Vediamo una conseguenza immediata del teorema appena citato.

Corollario 4.0.3. Il numero e^α è trascendente per ogni numero algebrico $\alpha \neq 0$. In particolare, se β è un numero reale algebrico diverso da 0 e 1, allora $ln(\beta)$ è trascendente.

Dimostrazione. Per il Teorema (4.0.2), se $\alpha \neq 0$ è algebrico, e^α non può essere radice di alcun polinomio a coefficienti razionali. Quindi e^α è un numero trascendente. Poiché $\beta = e^{ln(\beta)}$, vediamo anche che, se $ln(\beta) \neq 0$ è algebrico, allora β è trascendente. $\square$

Osservazione 4.0.4. Dato un qualsiasi $\alpha \neq 0$ algebrico, abbiamo che $\cos(\alpha)$, $\sin(\alpha)$ e $\tan(\alpha)$ sono trascendenti.

Dimostrazione. L'insieme dei numeri algebrici $\mathcal{A}$ è un campo. Sappiamo quindi che prodotti di elementi algebrici sono algebrici e dato α algebrico anche $\alpha \cdot i$ sarà algebrico.
Dalla formula di Eulero $e^{i\pi}+1=0$ abbiamo le seguenti:

$$\cos(\alpha) = \frac{e^{i\alpha} + e^{-i\alpha}}{2}$$
$$\sin(\alpha) = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}$$
$$\tan(\alpha) = \frac{e^{i\alpha} - e^{-i\alpha}}{i(e^{i\alpha} + e^{-i\alpha})}$$

Dimostriamo la trascendenza di ciascuno dei termini sopra.

- trascendenza di $\cos(\alpha)$: segue direttamente dal Teorema di Lindemann ponendo $\alpha_1 = \alpha \cdot i$ e $\alpha_2 = -\alpha \cdot i$.
- trascendenza di $\sin(\alpha)$: analogo al caso precedente.
- trascendenza di $\tan(\alpha)$: supponiamo per assurdo che dato α algebrico si abbia $\tan(\alpha)$ algebrico. Moltiplicando l'espressione $\tan(\alpha)$ per $\frac{e^{i\alpha}-e^{-i\alpha}}{e^{i\alpha}-e^{-i\alpha}}$ abbiamo che $\tan(\alpha) = -i \cdot \frac{e^{2i\alpha}-1}{e^{2i\alpha}+1}$. Tramite una serie di operazioni elementari otteniamo che $\frac{1}{e^{2i\alpha}} \in \mathcal{A}$. Ma, essendo $\mathcal{A}$ un campo, risulta che $e^{2i\alpha} \in \mathcal{A}$. Ciò contraddice il Corollario (4.0.3).

□

Osservazione 4.0.5. La trascendenza di e segue subito dal Teorema (4.0.2). La trascendenza di π segue dal Corollario (4.0.3). Infatti, se π fosse algebrico allora anche $\pi \cdot i$ sarebbe algebrico. Seguirebbe che $e^{i\pi}$ è trascendente. Ma $e^{i\pi} = -1$, si arriva così ad un assurdo.

Nelle successive due sezioni riportiamo semplici dimostrazioni dirette della trascendenza di e e π tratte da [8]. Tali dimostrazioni seguono le semplificazioni realizzate da D. Hilbert, A. Hurwitz e P. Gordan nel 1893 [10].

4.1 Trascendenza di e

Teorema 4.1.1. e è trascendente su $\mathbb{Q}$.

Dimostrazione. Siano $f \in \mathbb{Q}(x)$ un polinomio e t un numero complesso. Considerando l'integrale

$$\int_0^t e^{-u} f(u)du = [-e^{-u} f(u)]_0^t + \int_0^t e^{-u} f'(u)du$$

notiamo che è facilmente integrabile per parti.
Definiamo ora $I(t, f)$ in questo modo:

$$I(t, f) := \int_0^t e^{t-u} f(u) du$$

Allora abbiamo che

$$I(t, f) = e^t f(0) - f(t) + I(t, f')$$

Se f ha grado m, iterando la relazione sopra si ottiene la seguente:

$$I(t, f) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t) \tag{4.1}$$

Ponendo F come il polinomio ottenuto a partire da f sostituendo ciascun coefficiente di f con il suo valore assoluto, allora possiamo ottenere la seguente disuguaglianza (vedi [4, Lemma 4.3])

$$|I(t, f)| \leq |t| e^{|t|} F(|t|) \tag{4.2}$$

Formulate queste osservazioni, procediamo a dimostrare il teorema.

Per assurdo supponiamo che e sia algebrico su $\mathbb{Q}$ di grado n, cioè che è soluzione dell'equazione

$$a_n e^n + \cdots + a_1 e + a_0 = 0 \qquad (a_i \in \mathbb{Z}) \tag{4.3}$$

dove $a_0 a_n \neq 0$. Introduciamo ora il termine

$$J := \sum_{k=0}^{n} a_k I(k, f),$$

con

$$f(x) = x^{p-1}(x-1)^p (x-2)^p \ldots (x-n)^p$$

dove $p > |a_0|$ è un numero primo molto grande. Usando l'uguaglianza (4.3), notiamo che

$$J = -\sum_{j=0}^{m} \sum_{k=0}^{n} a_k f^{(j)}(k)$$

dove $m = (n+1)p - 1$. Poiché f ha uno zero di ordine p in $1, 2, \ldots, n$ e uno zero di ordine $p-1$ in 0, abbiamo che la prima sommatoria del termine J

inizia da $j = p - 1$.
Quando $j = p - 1$ il contributo di f è dato da

$$f^{(p-1)}(0) = (p-1)!(-1)^{np} n!^p$$

Dunque se $n < p$, allora $f^{(p-1)}(0)$ è divisibile per $(p-1)!$ ma non per p. Se $j \geq p$, vediamo che $f^{(j)}(0)$ e $f^{(j)}(k)$ sono divisibili per $p!$ quando $1 \leq k \leq n$. Ne segue che J è un intero diverso da zero divisibile per $(p-1)!$ e di conseguenza

$$(p-1)! \leq |J|$$

La stima (4.2) mostra che

$$|J| \leq \sum_{k=0}^{n} |a_k| e^k F(k) k \leq Ane^n((2n)!)^p$$

dove A è il massimo tra i valori assoluti dei termini a_k.
Otteniamo così la seguente:

$$(p-1)! \leq |J| \leq Ane^n((2n)!)^p$$

Dividendo i termini della disuguaglianza per $(p-1)!$ abbiamo che

$$1 \leq \frac{|J|}{(p-1)!} \leq \frac{Ane^n((2n)!)^p}{(p-1)!}$$

Per un primo p sufficientemente grande, si arriva ad una contraddizione.

□

4.2 Trascendenza di π

Per dimostrare la trascendenza di π sfruttiamo i lemmi che seguono.

Lemma 4.2.1. Se α è algebrico con polinomio minimo su $\mathbb{Z}$ dato da

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

allora anche $a_n \alpha$ è un intero algebrico, cioè è radice di un polinomio a coefficienti interi.

Dimostrazione. Moltiplicando $f(x)$ per a_n^{n-1} e valutandolo in α otteniamo la seguente:

$$f(\alpha) = (a_n \alpha)^n + a_{n-1}(a_n \alpha)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$$

Concludiamo così che $a_n \alpha$ è radice di un polinomio monico a coefficienti interi. □

Chiameremo *coniugati di* α le altre radici del polinomio minimo di α.

Lemma 4.2.2. Sia $f(x_1, \ldots, x_n)$ un polinomio simmetrico in $\mathbb{Q}[x_1, \ldots, x_n]$. Se α è algebrico di grado n con coniugati $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, allora $f(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Inoltre se α è un intero algebrico e $f \in \mathbb{Z}[x]$, allora $f(\alpha_1, \ldots, \alpha_n)$ è necessariamente un intero.

Dimostrazione. Si veda [8, Capitolo 3] □

Teorema 4.2.3. π è trascendente su $\mathbb{Q}$.

Dimostrazione. Procediamo per assurdo. Ponendo che π sia algebrico, allora anche $\alpha = i\pi$ è algebrico. Supponiamo che α abbia grado d e chiamiamo $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ i suoi coniugati. Sia N il coefficiente del termine di grado massimo nel polinomio minimo di α su $\mathbb{Z}$. Per quanto attesta il Lemma (4.2.1), $N\alpha$ è un intero algebrico. Inoltre, poiché

$$e^{i\pi} = -1$$

abbiamo

$$(1 + e^{\alpha_1})(1 + e^{\alpha_2}) \ldots (1 + e^{\alpha_d}) = 0$$

Questo prodotto può essere scritto come una somma di 2^d termini della forma e^θ, dove:

$$\theta = \epsilon_1\alpha_1 + \cdots + \epsilon_d\alpha_d, \quad \epsilon_i = 0, 1$$

Supponiamo che esattamente n di questi termini siano diversi da zero, e denotiamoli con $\beta_1, \ldots, \beta_n$. Osserviamo che questi β_i costituiscono tutte le radici di un polinomio a coefficienti interi. Per dimostrare questo fatto, notiamo che il polinomio

$$\prod_{\epsilon_1=0}^{1} \cdots \prod_{\epsilon_d=0}^{1} (x - (\epsilon_1\alpha_1 + \cdots + \epsilon_d\alpha_d)$$

è simmetrico in $\alpha_1, \ldots, \alpha_d$ e quindi appartiene a $\mathbb{Q}[x]$. Le radici di questo polinomio sono $\beta_1, \ldots, \beta_n$ e 0, che ha molteplicità $a = 2^d - n$. Dividendo per x^a ed eliminando il denominatore, otteniamo un polinomio in $\mathbb{Z}[x]$ con radici $\beta_1, \ldots, \beta_n$.
Ora

$$(1 + e^{\alpha_1})(1 + e^{\alpha_2}) \ldots (1 + e^{\alpha_d}) = 0$$

implica:

$$(2^d - n) + e^{\beta_1} + \cdots + e^{\beta_n} = 0$$

Utilizzando $I(t, f)$, definito come in (4.1.1), consideriamo la combinazione

$$K := I(\beta_1, f) + \cdots + I(\beta_n, f)$$

dove:

$$f(x) = N^{np} x^{p-1} (x - \beta_1)^p \dots (x - \beta_n)^p$$

e p denota un primo grande. Quindi

$$K = -(2^d - n) \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} \sum_{k=1}^{n} f^{(j)}(\beta_k)$$

dove $m = (n+1)p - 1$. La sommatoria su k è una funzione simmetrica in $N\beta_1, \dots, N\beta_n$. Osservando che $N\beta_1, \dots, N\beta_n$ sono le radici di un polinomio monico a coefficienti interi, concludiamo che tale somma è un intero. Inoltre, le derivate $f^{(j)}(\beta_k)$ si annullano per $j < p$, e la somma per $j \geq p$ è divisibile per $p!$. Per p sufficientemente grande abbiamo

$$f^{(p-1)}(0) = (p-1)!(-N)^{np}(\beta_1 \cdot \dots \cdot \beta_n)^p$$

che non è divisibile per p.
Procedendo in modo analogo a quanto fatto in (4.1.1), troviamo che:

$$|K| \leq \sum_{k=1}^{n} |\beta_k| e^{|\beta_k|} F(|\beta_k|) \leq AC^p$$

per certe costanti A e C. Sappiamo che K è un intero non nullo divisibile per $(p-1)!$.
Dunque, per un primo p sufficientemente grande si arriva ad una contraddizione. □

4.3 Indipendenza algebrica di e e π

Sebbene abbiamo dimostrato che π e e sono trascendenti su $\mathbb{Q}$, non è ancora noto se π è trascendente su $\mathbb{Q}(e)$ oppure se e è trascendente su $Q(\pi)$. A tal proposito, sono state sviluppate diverse considerazioni che riporteremo in questa sezione, concludendo con la *Congettura di Schanuel*.

Il teorema che segue, come accennato nel capitolo 3, ha portato alla risoluzione del settimo problema di Hilbert.

Teorema 4.3.1. (A. Gelfond-T. Schneider, 1934) Se α è un numero algebrico diverso da 0 e 1 e β è un numero irrazionale algebrico, allora α^β è trascendente.

Dimostrazione. Si veda [9]. □

Mediante il Teorema di Gelfond-Schneider è possibile dimostrare la trascendenza di numeri come e^{π}.

Corollario 4.3.2. e^{π} è un numero trascendente.

Dimostrazione. Per la *formula di Eulero* e^{ix}=cos(x)+$i$sin(x), risulta $e^{\pi} = i^{-2i}$, dove sia i che $-2i$ sono algebrici. Quindi possiamo applicare il Teorema (4.3.1). □

Osservazione 4.3.3. Non è ancora noto se α^{β} sia trascendente quando lo sono sia α che β. Ad esempio non è ancora noto se π^{e} sia trascendente.

L'insieme dei numeri trascendenti, diversamente da quello dei numeri algebrici, è chiuso per opposti e inversi, ma non per somma e prodotto.

Esempio 4.3.4. Dato α trascendente, il suo opposto e il suo inverso sono trascendenti. Infatti, se per assurdo $-\alpha$ fosse algebrico, allora $\alpha = -(-\alpha)$ sarebbe algebrico perchè l'insieme degli algebrici è chiuso per opposti. Analogamente, se per assurdo α^{-1} fosse algebrico, allora $\alpha = (\alpha^{-1})^{-1}$ sarebbe algebrico perchè l'insieme degli algebrici è chiuso per inversi.
Prendiamo banalmente $\alpha + (-\alpha) = 0$, oppure $\alpha \cdot \alpha^{-1} = 1$. In entrambi i casi otteniamo risultati algebrici.

Vediamo come si comportano e e π in questo contesto.

Osservazione 4.3.5. Se α e β sono trascendenti, almeno uno tra $\alpha + \beta$ e $\alpha \cdot \beta$ è trascendente. In particolare ciò vale per e e π.

Dimostrazione. Per assurdo, supponiamo che $\alpha + \beta$ e $\alpha \cdot \beta$ siano entrambi algebrici. Prendendo il polinomio

$$f(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

abbiamo che $f(x)$ ha coefficienti algebrici. Ciò implicherebbe che le radici di $f(x)$ sono numeri algebrici, ma α e β sono trascendenti. Si arriva così ad una contraddizione. □

Segue ora una delle più rilevanti osservazioni sollevate da S. Schanuel nell'ultimo secolo:

Congettura di Schanuel: Supponiamo che $\alpha_1, \ldots, \alpha_n$ siano numeri complessi linearmente indipendenti su $\mathbb{Q}$. Allora il grado di trascendenza di $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ su $\mathbb{Q}$ è almeno n.

Se tale congettura fosse verificata, se ne potrebbe dedurre immediatamente l'indipendenza algebrica su $\mathbb{Q}$ di $\{e, \pi\}$. Infatti consideriamo $\alpha_1 = 1$ e $\alpha_2 = i\pi$. Essi sono linearmente indipendenti su $\mathbb{Q}$ perchè $i\pi \notin \mathbb{Q}$. Calcolando gli esponenziali otteniamo i seguenti valori:

$$\alpha_1 = 1, \quad \alpha_2 = i\pi, \quad e^{\alpha_1} = e, \quad e^{\alpha_2} = -1$$

Segue dalla congettura che il grado di trascendenza su $\mathbb{Q}$ dell'insieme

$$\{1, i\pi, e, -1\}$$

è almeno 2. Poiché 1 e -1 sono numeri algebrici, π ed e sono necessariamente algebricamente indipendenti.

Bibliografia

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

[2] Stefania Gabelli. *Teoria delle equazioni e Teoria di Galois*. Springer, 2008.

[3] Patrick Morandi. *Fields and Galois Theory*. Springer, 1996.

[4] Marco Manetti. *Il quadrato non è tondo*, pag. 6-7. Sapienza Università di Roma, 2015. `https://www1.mat.uniroma1.it/people/manetti/spe2015/trascendenzapigreco.pdf`.

[5] D.J.H. Garling. *A course in Galois Theory*, cap 18. Cambridge University press, 1986.

[6] Alan Baker. *Transcendental Number Theory*, cap 1. Cambridge University press, 1975.

[7] Taha Rhaouti. *The transcendence of e and π*. Aprile 2023. `https://jonathanlove.info/teaching/23-NT/rhaouti.pdf`.

[8] M.Ram Murty. *Transcendental Numbers*. Springer, 2014.

[9] A. Gelfond. *Sur le septième problème de Hilbert*, pag. 624-630. Comptes Rendus Académie des Sciences de l'URSS e sul Bulletin de l'Académie des Sciences de l'URSS, 1934.

[10] P. Gordan. *Transcendencez von e und π*. Mathematische Annalen, vol.43, 1893.