Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

GLI AUTOMORFISMI DEL CAMPO DEI NUMERI COMPLESSI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
MARTA MORIGI

Presentata da:
DAVIDE MORIGI

Sessione III
Anno Accademico 2015/2016

Io non ho mai fatto niente di 'utile'.
Nessuna mia scoperta ha fatto o potrebbe
fare [...] *la minima differenza per*
la piacevolezza del mondo.
(G. H. Hardy)

Introduzione

Questo elaborato tratta di automorfismi, in particolare di automorfismi di campi. È risaputo, e di breve dimostrazione, che non esistono automorfismi del campo dei numeri razionali $\mathbb{Q}$ e del campo dei numeri reali $\mathbb{R}$ diversi dall'identità. Per quanto riguarda il campo complesso $\mathbb{C}$ invece, oltre all'identità, c'è un altro ben noto automorfismo, ovvero il coniugio complesso.
Fa inoltre parte del folklore matematico che esistano infiniti altri automorfismi del campo complesso. In questo elaborato, dunque, si fornisce una dimostrazione di tale fatto. Più in particolare si vanno ad analizzare tre proprietà caratteristiche degli automorfismi di $\mathbb{C}$, che andiamo qui di seguito brevemente ad elencare:

1. Ogni automorfimo di $\mathbb{C}$ diverso dall'identità e dal coniugio complesso fissa $\mathbb{Q}$ e manda $\mathbb{R} \setminus \mathbb{Q}$ in un sottoinsieme denso di $\mathbb{C}$.

2. Ogni automorfismo di un sottocampo di $\mathbb{C}$ può essere esteso a un automorfismo di $\mathbb{C}$ cioè, se F è un sottocampo di $\mathbb{C}$ e $\phi : F \to F$ è un automorfismo di F, allora esiste un automorfismo $\psi : \mathbb{C} \to \mathbb{C}$ di $\mathbb{C}$ tale che $\psi_{|F} = \phi$.

3. La cardinalità dell'insieme degli automorfismi di $\mathbb{C}$ è $2^{2^{\aleph_0}}$.

In realtà, a parte il punto 1, la cui dimostrazione sfrutta particolari caratteristiche topologiche proprie di $\mathbb{C}$, l'elaborato tratta in generale automorfismi di un campo algebricamente chiuso. I risultati ai punti 2 e 3 quindi continuano ad essere validi per un generico campo algebricamente chiuso Ω, ove la cardinalità dell'insieme degli automorfismi di Ω risulta essere $2^{\text{card } \Omega}$.

Per arrivare a dimostrare quest'ultimo punto sono necessari dei prerequisiti di insiemistica e dei risultati sulle basi di trascendenza. In particolare, siccome l'argomento non è stato trattato nei corsi di Algebra, nell'elaborato si dà particolare spazio e rilievo a una parte introduttiva sulle basi di trescendenza. Una volta presentate le principali proprietà di queste si va infine a dimostrare che, se Ω è un campo algebricamente chiuso, π il suo sottocampo fondamentale e B una base di trascendenza infinita di Ω su π, allora ogni permutazione degli elementi B induce un automorfismo di Ω. Questo, unito al fatto che $\text{card } B = \text{card } \pi(B) = \text{card } \Omega$, porta alla conclusione.
Poichè, come detto in precedenza, si è privilegiato un approccio il più generale possibile, si è analizzato separatamente il caso in cui la base di trascendenza B è finita. In ogni modo, anche se tramite altre argomentazioni, si giunge allo stesso risultato.

Indice

Capitolo 1

Risultati preliminari

1.1 Richiami di teoria dei campi

In questa prima sezione preliminare si esporranno risultati di teoria dei campi che saranno utili nel seguito della trattazione. La notazione utilizzata, ove non espressamente indicato, è quella standard. Data la mole di risultati necessari per avere un'idea precisa dell'argomento trattato, si è deciso di non mettere la dimostrazione di tutti i teoremi enunciati, privilegiando quelli non trattati nel corso di studi. In ogni caso, per le dimostrazioni non presenti, si può fare riferimento al libro *Algebra* di T. Hungerford.

Definizione 1.1. Sia $F \subseteq K$ un'estensione di campi e siano $\alpha_1, \alpha_2, ..., \alpha_n \in K$. L'intersezione di tutti i sottocampi di K contenenti $F, \alpha_1, \alpha_2, ..., \alpha_n$ si indica con $F(\alpha_1, \alpha_2, ..., \alpha_n)$ ed è chiamata *campo di estensione* di F generato da $\alpha_1, \alpha_2, ..., \alpha_n$. I numeri $\alpha_1, \alpha_2, ..., \alpha_n$ sono detti *generatori* di $F(\alpha_1, ..., \alpha_n)$.
Se G è un campo che contiene F, con $G = F(\beta_1, \beta_2, ..., \beta_k)$ per un certo insieme finito di numeri $\beta_1, \beta_2, ...\beta_k$, si dice che G è un'*estensione finitamente generata* di F.
Se $G = F(\beta)$, si dice che G è un'*estensione semplice* di F.

Definizione 1.2. Sia $F \subseteq K$ un'estensione di campi. Un elemento $\alpha \in K$ si dice *algebrico* su F se esiste un polinomio $p(x) \in F[x]$ tale che $p(\alpha)$=0.

Se questo non succede, α si dice *trascendente* su F.

Proposizione 1.3. *Sia $F \subseteq K$ un'estensione di campi, $\alpha \in K$. Allora esiste un unico polinomio monico irriducibile $p(x) \in F[x]$ tale che $p(\alpha)=0$. Inoltre se $q(x) \in F[x]$ è tale che $q(\alpha)=0$, allora si ha che $p(x)$ divide $q(x)$. Il polinomio $p(x)$ si dice polinomio minimo di α su F.*

Proposizione 1.4. *Sia $F \subseteq K$ e sia $\alpha \in K$. Consideriamo il morfismo di valutazione in α:*

$$\begin{array}{rccc} \phi_\alpha : & F[x] & \to & K \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

e l'isomorfismo indotto da ϕ_α:

$$\begin{array}{rccc} \psi : & F[x]/\ker\phi_\alpha & \to & F[\alpha] \\ & \overline{f(x)} & \mapsto & f(\alpha) \end{array}$$

Allora:

- *se α è algebrico su F, cioè $\ker\phi_\alpha = (p_\alpha)$, dove p_α è il polinomio minimo di α su F, si ha che $F[\alpha] = F(\alpha)$ è isomorfo a $F[x]/(p_\alpha)$;*
- *se α è trascendente su F, cioè $\ker\phi_\alpha = (0)$, si ha che $F[\alpha]$ è isomorfo a $F[x]$ e $F(\alpha)$ è isomorfo a $F(x)$.*

Definizione 1.5. Sia $F \subseteq K$ un'estensione di campi.

- $F \subseteq K$ si dice *algebrica* se ogni elemento di K è algebrico su F;
- $F \subseteq K$ si dice *finita* se la dimensione di K come F-spazio vettoriale è finita; tale dimensione è indicata con $[K : F]$ e si dice grado di K su F.

Proposizione 1.6. *Siano $F \subseteq K$, $K \subseteq L$ estensioni di campi algebriche. Allora $F \subseteq L$ è algebrica.*

Proposizione 1.7. *Sia $F \subseteq K$ un'estensione di campi finita. Allora:*

1. *esistono* $\alpha_1, ..., \alpha_n \in K$ *tali che* $K = F(\alpha_1, ..., \alpha_n)$*;*

2. $F \subseteq K$ *è un'estensione algebrica.*

Proposizione 1.8. *Sia* $F \subseteq K$ *un'estensione di campi e sia* $\alpha \in K$ *algebrico su* F*. Sia* p_α *il polinomio minimo di* α *su* F*. Allora si ha che la dimensione di* $F[\alpha]$ *come* F*-spazio vettoriale è pari al grado di* p_α*.*

Definizione 1.9. Sia F un campo. F si dice *algebricamente chiuso* se ogni polinomio $p(x) \in F[x]$ di grado ≥ 1 ha una radice in F o, equivalentemente, se ogni polinomio $p(x) \in F[x]$ si fattorizza in fattori lineari in $F[x]$.

Definizione 1.10. Un campo Ω si dice una *chiusura algebrica* di un suo sottocampo K se $K \subseteq \Omega$ è un'estensione algebrica e Ω è algebricamente chiuso.

Teorema 1.11. *Ogni campo* K *ha una chiusura algebrica* Ω*. Inlotre, se* Ω_1*,* Ω_2 *sono due chiusure algebriche di* K*, allora esiste un isomorfismo di campi tra* Ω_1 *e* Ω_2 *che induce l'identità su* K*.*

Definizione 1.12. Sia $F \subseteq K$ un'estensione di campi e sia $\mathcal{S}$ un sottoinsieme di K. Il più piccolo sottoanello di K che contiene F e $\mathcal{S}$ (o, equivalentemente, l'intersezione di tutti i sottoanelli che contengono F) si dice *generato* da F e $\mathcal{S}$. Nel seguito esso verrà denotato con $F[\mathcal{S}]$.

Osservazione 1.13. Con le notazioni della definizione precedente, risulta che $F[\mathcal{S}]$ consiste dell'insieme degli elementi di K che possono essere scritti come somma finita nella forma

$$\sum a_{i_1,...,i_n} \alpha_1^{i_1} \cdot ... \cdot \alpha_n^{i_n}$$

ove $a_{i_1,...,i_n} \in F$, $\alpha_i \in \mathcal{S}$ per $i = 1, ..., n$.

Dimostrazione. Sia

$$R = \{\sum a_{i_1,...,i_n} \alpha_1^{i_1} \cdot ... \cdot \alpha_n^{i_n} \text{ t.c. } a_{i_1,...,i_n} \in F, \alpha_i \in \mathcal{S} \text{ per } i = 1, ..., n\}$$

È semplice verificare che R è un anello che contiene F e $\mathcal{S}$ e che è contenuto in un qualsiasi anello che contiene F e $\mathcal{S}$. Quindi $R = F[\mathcal{S}]$. □

Lemma 1.14. ***(della Torre)*** *Siano F,G,K campi, con $F \subseteq G \subseteq K$. Allora si ha che $F \subseteq K$ è finita se e solo se $F \subseteq G$ e $G \subseteq K$ sono finite. In questo caso vale $[K : F] = [K : G]\,[G : F]$.*

Teorema 1.15. *Sia $K \subseteq F$ un'estensione di campi e sia X un sottoinsieme di F tale che $F = K(X)$, ove ogni elemento $x \in X$ è algebrico su K. Allora F è un'estensione algebrica di K.*

Dimostrazione. Se $v \in F = K(X)$ allora, per l'Osservazione 1.13, esistono $u_1, ..., u_n \in X$ tali che $v \in K(u_1, ..., u_n)$. Andiamo a considerare ora la catena di campi $K \subseteq K(u_1) \subseteq K(u_1, u_2) \subseteq ... \subseteq K(u_1, ..., u_n)$. Siccome u_i è algebrico su K per ogni $i = 1, ..., n$, allora è in particolare algebrico su $K(u_1, ..., u_{i-1})$ per $i > 1$. Siano $r_1 = [K(u_1) : K]$ e $r_i = [K(u_1, ..., u_i) : K(u_1, ..., u_{i-1})]$ per $i = 2, ..., n$. Allora, applicando iterativamente il Lemma della Torre, si ha che $[K(u_1, ..., u_n) : K] = r_1 \cdot ... \cdot r_n$. Dunque, per la Proposizione 1.7, si ha che $K \subset K(u_1, ..., u_n)$ è algebrica. Allora, siccome $v \in K(u_1, ..., u_n)$, v è algebrico su K. Questo, data l'arbitrarietà di $v \in F$, conclude la dimostrazione. □

Teorema 1.16. *Sia $F \subseteq K$ un'estensione di campi. Allora*

$$\overline{F} = \{\alpha \in K \text{ tali che } \alpha \text{ è algebrico su } F\}$$

è un campo.

Dimostrazione. Siano $\alpha, \beta \in \overline{F}$. Dobbiamo far vedere che $-\alpha, \alpha\beta, \alpha + \beta$ e, se $\alpha \neq 0$, $\frac{1}{\alpha}$ appartengono a $\overline{F}$.
Abbiamo $\overline{F}\,[\alpha] = \overline{F}(\alpha)$. Siccome α è algebrico su $\overline{F}$, vale $\left[\overline{F}(\alpha) : \overline{F}\right] < \infty$, $\left[\overline{F}(\alpha, \beta) : \overline{\overline{F}}(\alpha)\right] < \infty$. Quindi, per il Lemma della Torre, risulta che $\left[\overline{F}(\alpha, \beta) : \overline{F}\right] < \infty$; dunque, se $\gamma \in \overline{F}$, si ha che $[F(\gamma) : F] < \infty$ (in quanto $\left[\overline{F}(\alpha, \beta) : \overline{F}\right] = \left[\overline{F}(\alpha, \beta) : \overline{F}(\gamma)\right]\left[\overline{F}(\gamma) : \overline{F}\right]$). Allora γ è algebrico su $\overline{F}$.
Prendendo $\gamma = \alpha + \beta$, $\gamma = \frac{1}{\alpha}$, $\gamma = \alpha\beta$, $\gamma = -\alpha$ si ha la tesi, in quanto tutti questi elementi appartengono a $\overline{F}(\alpha, \beta)$. □

Definizione 1.17. Siano K un campo e $t \in \mathbb{Z}^+$. Poniamo $t1_K = 1_K + ... + 1_K$ (t addendi).

- Se esiste $t \in \mathbb{Z}^+$ tale che $t1_K = 0$, allora si definisce la caratteristica di K come car $K = \min\{t \in \mathbb{Z}^+ \text{ t.c. } t1_K = 0\}$
- Se $t1_K \neq 0$ per ogni $t \in \mathbb{Z}^+$, allora si pone car $K = 0$

Definizione 1.18. Sia K un campo. Il più piccolo sottocampo contenuto in K o, equivalentemententente, l'intersezione di tutti i sottocampi contenuti in K, si dice *sottocampo fondamentale di K.*

Teorema 1.19. *Sia K un campo. Allora il suo sottocampo fondamentale è:*

- $\mathbb{Z}_p$ *se* car *K=p;*
- $\mathbb{Q}$ *se* car *K=0.*

Teorema 1.20. ***(Criterio di Eisentein)*** *Sia* $f(x) = a_0 + ... + a_n x^n \in \mathbb{Z}[x]$. *Se esiste un primo p tale che:*

1. $p \nmid a_n$
2. $p \mid a_0, ..., p \mid a_{n-1}$
3. $p^2 \nmid a_0$

Allora $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$.

Corollario 1.21. *Per ogni* $n \in \mathbb{Z}^+$ *esiste un polinomio irriducibile in* $\mathbb{Q}[x]$ *di grado n. Infatti basta considerare, per esempio, il polinomio* $f(x) = x^n + 3$ *e verificare che esso soddisfa le ipotesi del Criterio di Eisentein.*

Teorema 1.22. *Sia F un campo con q elementi e sia* $n \in \mathbb{Z}^+$. *Allora esiste almeno un'estensione di F di grado n.*

Corollario 1.23. *Sia F un campo finito. Allora per ogni* $n \in \mathbb{Z}^+$ *esiste almeno un polinomio irriducibile* $f(x) \in F[x]$ *di grado n.*

1.2 Estensioni trascendenti di campi

In questa seconda sezione introduttiva si discuterà brevemente che cos'è una base di trascendenza e che cos'è un'ampliamento trascendente di campi, e darà le proprietà fondamentali di tali ampliamenti. Infatti questi strumenti saranno indispensabili nello sviluppo dell'ultimo capitolo di questa tesi, quello legato alla cardinalità dell'insieme degli automorfismi del campo dei numeri complessi.

Definizione 1.24. Sia $F \subseteq K$ un'estensione di campi e siano $\alpha_1, ..., \alpha_n \in K$. Posto $\alpha = (\alpha_1, ..., \alpha_n)$ e $F[x] = F[x_1, ...x_n]$, consideriamo il morfismo di valutazione:

$$\begin{array}{rccc} \nu_\alpha : & F[x] & \to & K \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

Gli elementi $\alpha_1, ..., \alpha_n$ si dicono *algebricamente indipendenti su* F se $\ker(\nu_\alpha) = (0)$. Altrimenti essi si dicono *algebricamente dipendenti*. In altre parole $\alpha_1, ...\alpha_n$ sono algebricamente dipendenti su F se esiste un polinomio di grado positivo $f(x_1, ..., x_n) \in F[x]$ tale che $f(\alpha_1, ..., \alpha_n) = 0$. In questo caso l'uguaglianza $f(\alpha_1, ..., \alpha_n) = 0$ si dice una *relazione algebrica su* $\alpha_1, ..., \alpha_n$ (a coefficienti in F).

Osservazione 1.25. Segue dalla definizione che se n elementi di K sono algebricamente indipendenti su F, allora lo sono anche s elementi comunque scelti fra essi.

Definizione 1.26. Un sottoinsieme $\mathcal{S}$ di K si dice *algebricamente indipendente su* F se ogni suo sottoinsieme finito è costituito da elementi algebricamente indipendenti su F.

Osservazione 1.27. Applicando la definizione al caso *n=1*, si ha che α è algebricamente indipendente su F se e soltanto se è trascendente su F. Quindi elementi indipendenti su F sono trascendenti. Tuttavia, se $\alpha_1, ..., \alpha_n$ sono trascendenti su F, essi possono essere algebricamente dipendenti. Ad esempio

π e π^2 sono entrambi trascendenti su $\mathbb{Q}$ ma, se si considera $f(x_1, x_2) = x_1^2 - x_2$, risulta $f(\pi, \pi^2) = 0$. Dunque π e π^2 sono algebricamente dipendenti su $\mathbb{Q}$.

Proposizione 1.28. *Sia $F \subseteq K$ un'estensione di campi. Gli elementi $\alpha_1, ..., \alpha_n \in K$ sono algebricamente indipendenti su F se e soltanto se α_1 è trascendente su F e α_i è trascendente su $F(\alpha_1, ..., \alpha_{i-1})$ per i=2,...,n.*

Dimostrazione. Basta osservare che α_i è algebrico su $F(\alpha_1, ..., \alpha_{i-1})$ se e soltanto se esiste un polinomio di grado positivo $f(x) \in F(\alpha_1, ..., \alpha_{i-1})[x]$ tale che $f(\alpha_i) = 0$. Ma ciò equivale a dire che esiste un polinomio di grado positivo $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ tale che $f(\alpha_1, ..., \alpha_i) = 0$, ovvero che $\alpha_1, ..., \alpha_i$ sono algebricamente dipendenti su F. □

Proposizione 1.29. *Sia $F \subseteq K$ un'estensione di campi. Gli elementi $\alpha_1, ..., \alpha_n \in K$ sono algebricamente indipendenti su F se e solamente se l'applicazione*

$$\begin{array}{rccc} \nu'_\alpha : & F(x_1, ..., x_n) & \to & F(\alpha_1, ..., \alpha_n) \\ & \frac{f(x_1,...,x_n)}{g(x_1,...,x_n)} & \mapsto & \frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} \end{array}$$

è un F-isomorfismo.

Dimostrazione. Per definizione $\alpha_1, ..., \alpha_n$ sono algebricamente indipendenti su F se e soltanto se l'omomorfismo $\nu_\alpha : F[x_1, ..., x_n] \to K$ è iniettivo, ovvero se la sua immagine

$$F[\alpha] = \{f(\alpha_1, ..., \alpha_n) \text{ t.c. } f(x_1, ..., x_n) \in F[x_1, ..., x_n]\}$$

è un anello isomorfo a $F[x_1, ..., x_n]$. In questo caso è di facile verifica che ν_α si estende ad un F-isomorfismo $\nu'_\alpha : F(x_1, ..., x_n) \to F(\alpha_1, ..., \alpha_n)$ ponendo $\nu'_\alpha(\frac{f(x_1,...,x_n)}{g(x_1,...,x_n)}) = \frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)}$.

Viceversa, se ν'_α è un isomorfismo, allora $\ker(\nu'_\alpha) = (0)$, cioè $\alpha_1, ..., \alpha_n$ non possono annullare nessun polinomio di grado positivo in $x_1, ..., x_n$ a coefficienti in F. □

Definizione 1.30. Si dice che l'estensione di campi $F \subseteq K$ è *puramente trascendente* se $K = F(\mathcal{S})$ per qualche sottoinsieme $\mathcal{S}$ di K algebricamente indipendente su F. In particolare, un ampliamento finitamente generato $F(\alpha_1, ...\alpha_n)$ è puramente trascendente se gli elementi $\alpha_1, ..., \alpha_n$ sono algebricamente indipendenti su F o, equivalentemente (per la Proposizione 1.29), se $F(\alpha_1, ..., \alpha_n)$ è isomorfo al campo delle funzioni razionali $F(x_1, ..., x_n)$. Un ampliamento semplice $F(\alpha)$ di F o è algebrico oppure è puramente trascendente su F, e questa seconda eventualità si verifica esattamente quando α è trascendente su F. In quest'ultimo caso si dice che $F(\alpha)$ è un *ampliamento semplice trascendente di F*.

Definizione 1.31. Data un'estensione di campi $F \subseteq K$, un sottoinsieme $\mathcal{S}$ di K si dice una *base di trascendenza di K su F* se l'ampliamento $F \subseteq F(\mathcal{S})$ è puramente trascendente ed inoltre se K è algebrico su $F(\mathcal{S})$. In particolare, se $K = F(\mathcal{S})$ è un ampliamento puramente trascendente, allora $\mathcal{S}$ è una base di trascendenza di K su F.

Definizione 1.32. Sia $\Im$ un insieme parzialmente ordinato, $Q \subseteq \Im$. Si dice *maggiorante* di Q un elemento $q \in Q$ tale che $p \leq q$ per ogni $p \in Q$.

Definizione 1.33. Sia $\Im$ un insieme parzialmente ordinato, $Q \in \Im$. Si dice che m è un elemento *massimale* di Q se per ogni $q \in Q$, se $q \geq m$, allora $q = m$.

Definizione 1.34. Sia $\Im$ un insieme parzialmente ordinato. $\zeta \in \Im$ si dice *catena* se $\zeta \neq \emptyset$ e, per ogni $a, b \in \zeta$, vale $a \leq b$ oppure $b \leq a$, cioè ogni coppia di elementi di ζ è confrontabile.

Si enuncia ora un teorema fondamentale, della cui dimostrazione si darà solamente un'idea generale. Per farlo introduciamo uno strumento che useremo molto nel corso della trattazione, ovvero il Lemma di Zorn.

Lemma di Zorn. Sia $\Im$ un insieme non vuoto su cui è definita una relazione d'ordine parziale. Se ogni sottoinsieme totalmente ordinato di $\Im$ ha un maggiorante in $\Im$, allora $\Im$ ha un elemento massimale.

Teorema 1.35. *Sia $F \subseteq K$ un'estensione di campi non algebrica. Allora esiste una base di trascendenza di K su F.*

Dimostrazione. L'esistenza di una tale base di trascendenza è assicurata dal Lemma di Zorn. Infatti, l'insieme di tutti i sottoinsiemi di K algebricamente indipendenti su F è parzialmente ordinato per inclusione ed ogni catena di questo insieme ammette un maggiorante, dato dall'unione degli insiemi della catena. Dunque esiste un sottoinsieme $\mathcal{S}$ di K massimale rispetto alla proprietà di essere algebricamente indipendente su F, e questo è una base di trascendenza di K su F, poichè risulta che K è algebrico su $F(\mathcal{S})$. □

Teorema 1.36. *Sia $F \subseteq K$ un'estensione di campi. Supponiamo che K abbia una base di trascendenza finita $\{\beta_1, ..., \beta_n\}$ su F. Se $\alpha_1, ..., \alpha_m \in K$ sono algebricamente indipendenti su F, allora $m \leq n$ e si può completare l'insieme $\{\alpha_1, ..., \alpha_m\}$ a una base di trascendenza aggiungendo al più n-m elementi di $\{\beta_1, ..., \beta_n\}$. In particolare, il numero degli elementi di una base di trascendenza di K su F è il massimo numero di elementi di K algebricamente indipendenti su F.*

Dimostrazione. Se $\{\beta_1, ..., \beta_n\}$ è una base di trascendenza di K su F, allora α_1 è algebrico su $L = F(\beta_1, ..., \beta_n)$. Quindi esiste un polinomio di grado positivo $f(x) = c_0 + c_1x + ... + c_sx^s \in L[x]$ tale che $f(\alpha_1) = 0$. Questa è una relazione algebrica che coinvolge α_1 e gli elementi di $\{\beta_1, ..., \beta_n\}$ che compaiono nei coefficienti di $f(x)$ (che non appartengono tutti ad F in quanto α_1 è trascendente su F). Supponiamo, senza perdita di generalità, che β_1 compaia nei coefficienti di $f(x)$. Allora, considerando $f(x)$ come polinomio in β_1, si avrà che β_1 è algebrico su $L' = F(\alpha_1, \beta_2, ..., \beta_n)$. Consideriamo le inclusioni di campi $L' \subseteq L'(\beta_1) = L(\alpha_1) \subseteq K$. Osservviamo ora che $L' \subseteq L'(\beta_1)$ e $L(\alpha_1) \subseteq K$ sono estensione algebriche. Infatti la prima è algebrica per quanto appena detto, mentre la seconda lo è in quanto $L \subseteq K$ è algebrica. Dunque si ha che K è un'estensione algebrica di $L' = F(\alpha_1, \beta_2, ..., \beta_n)$. Se $m \leq n$ si può iterare questo procedimento ed ottenere che K è algebrico su $F(\alpha_1, ..., \alpha_m, \beta_{m+1}, ..., \beta_n)$. D'altra parte non può essere $m > n$, altrimenti

α_{n+1} sarebbe algebrico su $F(\alpha_1, ..., \alpha_n)$. Infatti possiamo iterare il procedimento descritto sopra senza problemi per n passi e, arrivati a quel punto, avremmo che K è algebrico su $F(\alpha_1, ..., \alpha_n)$. Ma non è possibile che α_{n+1} sia algebrico su $F(\alpha_1, ..., \alpha_n)$ in quanto per ipotesi $\alpha_1, ..., \alpha_m$ sono algebricamente indipendenti. □

Corollario 1.37. *Sia $F \subseteq K$ un'estensione di campi. Se esiste una base di trascendenza finita $\mathcal{S}$ di K su F e $\mathcal{T}$ è un'altra base di trascendenza di K su F, allora $\mathcal{S}$ e $\mathcal{T}$ hanno lo stesso numero di elementi.*

Osservazione 1.38. Anche nel caso infinito si può dimostrare che due basi di trascendenza hanno lo stesso numero di elementi, quindi in ogni caso si può definire il grado di trascendenza di un'estensione $F \subseteq K$ come la cardinalità di una qualsiasi base di trascendenza di K su F. Siccome però non si è ancora data alcuna definizione di cardinalità di un insieme infinito, cosa che si farà nella prossima parte introduttiva, la dimostrazione di questo risultato verrà data nel secondo capitolo.

Definizione 1.39. Possiamo a questo punto definire il *grado di trascendenza* di un'estensione di campi $F \subseteq K$ nel seguente modo:

- Se K è algebrico su F, il suo grado di trascendenza su F è 0;
- Se K ha una base di trascendenza finita su F, il suo grado di trascendenza su F è il numero degli elementi di tale base (ovvero il massimo numero di elementi di K algebricamente indipendenti su F);
- Se K ha una base di trascendenza infinita, il suo grado di trascendenza su F è infinito.

Indicheremo il grado di trascendenza con $\mathrm{trdeg}_F(K)$.

1.3 Sulla cardinalità di insiemi

Sono nel seguito elencati alcuni risultati di insiemistica, indispensabili per comprendere l'ultima parte della trattazione sulla cardinalità dell'insieme degli automorfismi di $\mathbb{C}$.

Definizione 1.40. Due insiemi, A e B, si dicono *equipotenti* se esiste un'applicazione biiettiva $A \to B$.

Osservazione 1.41. Sia $\mathcal{F}$ la famiglia di tutti gli insiemi. Allora si verifica facilmente che l'equipotenza gode delle seguenti proprietà:

1. A è equipotente ad A per ogni $A \in \mathcal{F}$;
2. se A è equipotente a B, allora B è equipotente ad A per ogni $A, B \in \mathcal{F}$;
3. se A è equipotente a B e B è equipotente a C, allora A è equipotente a C per ogni $A, B, C \in \mathcal{F}$.

Definizione 1.42. La *cardinalità* (o *numero cardinale*) di un insieme A, denotata da card A o da $|A|$, è la classe di equivalenza di A nella relazione di equipotenza. $|A|$ è finita o infinita a seconda che A sia rispettivamente finito o infinito.

Osservazione 1.43. La cardinalità di un insieme è spesso denotata con le lettere greche $\alpha, \beta, ...$ Valgono le seguenti proprietà:

1. Ogni insieme ha un unico numero cardinale.
2. Due insiemi hanno lo stesso numero cardinale se e solo se sono equipotenti.

Esempio 1.44. La cardinalità dell'insieme dei numeri naturali $\mathbb{N}$ viene indicata con $\aleph_0$.

Definizione 1.45. Siano α e β numeri cardinali e A, B insiemi tali che $|A| = \alpha$, $|B| = \beta$. Si dice che $\alpha \leq \beta$ se esiste una mappa iniettiva $A \to B$ (cioè A è equipotente a un sottoinsieme di B). Si dice che $\alpha < \beta$ se $\alpha \leq \beta$ e $\alpha \neq \beta$.

Definizione 1.46. Siano α e β numeri cardinali e A, B insiemi tali che $|A| = \alpha$, $|B| = \beta$, con $A \cap B = \emptyset$. La somma $\alpha + \beta$ è definita dal numero cardinale $|A \cup B|$. Il prodotto $\alpha\beta$ è definito dal numero cardinale $|A \times B|$.

Proposizione 1.47. *Se A è un insieme e $\mathcal{P}(A)$ è il suo insieme delle parti, allora* card $A <$ card $\mathcal{P}(A)$. *Si pone* card $\mathcal{P}(A) = 2^{\text{card } A}$.

Teorema 1.48. *Ogni insieme infinito ha un sottoinsieme numerabile. In particolare, risulta $\aleph_0 \leq \alpha$ per ogni numero cardinale infinito α.*

Lemma 1.49. *Siano A un insieme infinito e F un insieme finito. Allora $|A \cup F| = |A|$.*

Teorema 1.50. *Siano α, β numeri cardinali tali che $\beta \leq \alpha$, con α infinito. Allora $\alpha + \beta = \alpha$.*

Teorema 1.51. *Siano α, β numeri cardinali tali che $\beta \leq \alpha$, con α infinito. Allora $\alpha\beta = \alpha$; in particolare $\alpha\aleph_0 = \alpha$ e, se β è finito, allora $\beta\aleph_0 = \aleph_0$.*

Teorema 1.52. *Sia A un insieme e sia $A^n = A \times A \times ... \times A$ (n fattori) per ogni $n \geq 1$. Allora:*

1. *Se A è finito vale $|A^n| = |A|^n$ e, se A è infinito, risulta $|A^n| = |A|$.*
2. $|\bigcup_{n \in \mathbb{N}^*} A^n| = \aleph_0 |A|$.

Teorema 1.53. *Sia S un insieme infinito. Sia $(A_n)_{n \in \mathbb{N}}$ una famiglia di insiemi disgiunti con la stessa cardinalità di S. Allora $|\bigcup_{n \in \mathbb{N}} A_n| = |S|$.*

Dimostrazione. Sicuramente vale $|S| \leq |\bigcup_{n \in \mathbb{N}} A_n|$ in quanto, fissato $m \in \mathbb{N}$, vale $|S| = |A_m| \leq |\bigcup_{n \in \mathbb{N}} A_n|$.
Per ipotesi sappiamo che per ogni $n \in \mathbb{N}$ esiste una biiezione $\varphi_n : A_n \to S$. Consideriamo la mappa

$$\begin{array}{rccc} \phi : & \bigcup_{n \in \mathbb{N}} A_n & \to & \mathbb{N} \times S \\ & a & \mapsto & (i, \varphi_i(a)) \end{array}$$

Siccome $A_i \cap A_j = \emptyset$ per $i \neq j$ si ha che ϕ è una mappa ben definita. Inoltre ϕ è iniettiva, e dunque vale $|\bigcup_{n\in\mathbb{N}} A_n| \leq |\mathbb{N} \times S| = \aleph_0 \times |S| = |S|$, ove l'ultima uguaglianza vale per il Teorema 1.51, siccome S è infinito. □

Teorema 1.54. *Sia $K \subseteq F$ un'estensione di campi algebrica. Allora $|F| \leq \aleph_0|K|$.*

Dimostrazione. Sia T l'insieme di tutti i polinomi di grado positivo appartenenti a $K[x]$. Mostriamo innanzitutto che $|T| = \aleph_0|K|$.
Per ogni $n \in \mathbb{N}^*$ sia T_n l'insieme di tutti i polinomi di grado n. Allora risulta $T = \bigcup_{n\in\mathbb{N}^*} T_n$. Dunque, se consideriamo l'applicazione $\varphi_n : T_n \to K^n$ tale che $\varphi_n(x^n + a_{n-1}x^{n-1} + ... + a_0) = (a_0, ..., a_{n-1})$, si ha che questa è una biiezione, perciò $|T_n| = |K^n|$. Poichè gli insiemi T_n (rispettivamente K_n) sono a due a due disgiunti, la mappa

$$\begin{array}{rccc} f: & T = \bigcup\limits_{n\in\mathbb{N}^*} T_n & \to & \bigcup\limits_{n\in\mathbb{N}^*} K^n \\ & u & \mapsto & \varphi_n(u) \end{array}$$

dove $u \in T_n$, è una biiezione ben definita. Quindi $|T| = |\bigcup_{n\in\mathbb{N}^*} K^n| = \aleph_0|K|$ per il Teorema 1.52.
Ora mostriamo che $|F| \leq |T|$, il che completerà la dimostrazione. Per ogni polinomio irriducibile $f \in T$, scegliamo un ordinamento delle radici distinte di f in F. Definiamo una mappa $F \to T \times \mathbb{N}^*$ come segue:
se $\alpha \in F$, allora α è algebrico su K per ipotesi e quindi, per la Proposizione 1.3, esiste un unico polinomio monico irriducibile $p \in T$ tale che $p(\alpha) = 0$. Assegnamo ad $\alpha \in F$ la coppia $(p, i) \in T \times \mathbb{N}^*$ dove α è la i-esima radice nell'ordinamento delle radici di p in F precedentemente scelto. Non è difficile verificare che questa mappa $F \to T \times \mathbb{N}^*$ è ben definita e iniettiva. Poichè T è infinito, allora $|F| \leq |T \times \mathbb{N}^*| = |T||\mathbb{N}^*| = \aleph_0|T| = |T|$, ove l'ultima uguaglianza vale per il Teorema 1.51.

□

Teorema 1.55. *Sia $F \subseteq K$ un'estensione di campi. Supponiamo esista una base di trascendenza finita S di K su F. Allora vale $|F(S)| = |F|$.*

Dimostrazione. Sia $S = \{\lambda_1, \lambda_2, ..., \lambda_n\}$. Facciamo la dimostrazione per induzione su n.

- PASSO BASE: se $n = 1$, allora si ha che $S = \{\lambda_1\}$. Per la Proposizione 1.4 sappiamo che $F(\lambda_1) \cong F(x_1)$, dove x_1 è un'indeterminata; quindi $|F(\lambda_1)| = |F(x_1)|$. Inoltre $|F(x_1)| = |F[x_1]|$. Infatti $F(x_1) = F[x_1] \times F[x_1]/_\sim$, dove $(f, g) \sim (h, s)$ se e solo se $fs = hg$. Quindi si ha che $|F(x_1)| = |F[x_1] \times F[x_1]/_\sim| \leq |F[x_1] \times F[x_1]| =$ (per il Teorema 1.52) $= |F[x_1]|$. Poichè $F(x_1) \supset F[x_1]$, allora $|F(x_1)| \geq |F[x_1]|$. Dunque si ha $|F(x_1)| = |F[x_1]|$. Consideriamo ora l'applicazione:

$$\begin{array}{rccc} \varphi: & F[x_1] & \to & \bigcup\limits_{n\in\mathbb{N}^*} F^n \\ & a_0 + a_1x_1 + ... + a_nx_1^n & \mapsto & (a_0, a_1, ..., a_n) \end{array}$$

  Chiaramente φ è una biiezione; inlotre, per il Teorema 1.52, si ha che $|\bigcup\limits_{n\in\mathbb{N}^*} F^n| = |F|$ e dunque $|F[x_1]| = |F|$. Quindi $|F(x_1)| = |F|$.

- PASSO INDUTTIVO: supponiamo vera l'affermzione per n e dimostramola per *n+1*. Per ipotesi induttiva sappiamo che $|F(\lambda_1, ..., \lambda_n)| = |F|$. Poniamo $L = F(\lambda_1, ..., \lambda_n)$. Allora, per il passo base sappiamo che $|L(\lambda_{n+1})| = |L|$. Dunque si ha che $|F(\lambda_1, ..., \lambda_{n+1})| = |L(\lambda_{n+1})| = |L| = |F(\lambda_1, ..., \lambda_n)| = |F|$, il che conclude la dimostrazione.

□

Lemma 1.56. *Sia A un insieme infinito e sia Λ l'insieme di tutti i suoi sottoinsiemi finiti. Allora vale* card $A =$ card Λ.

Dimostrazione. Iniziamo innanzitutto col mostrare che, se Λ_n è l'insieme di tutti i sottoinsiemi di A di cardinalità minore o uguale di n, allora si ha che card $A =$ card Λ_n.
Sicuramente card $A \leq$ card Λ_n (è sufficiente considerare l'applicazione $\varphi : A \to \Lambda_n$ tale che $\varphi(a) = \{a\}$) e, quindi, card $A \leq$ card $\Lambda_n \leq$ card Λ.
Inlotre, se consideriamo $\varphi : A^n \to \Lambda_n$ tale che $\varphi(a_1, ..., a_n) = \{a_1, ..., a_n\}$, si

ha che φ è suriettiva. Quindi $|\Lambda_n| \leq |A^n| = |A|$ per in Teorema 1.52. Quindi $|A| = |\Lambda_n|$. Si ha che $\Lambda = \bigcup_{n\in\mathbb{N}} \Lambda_n$ e quindi, sempre per il Teorema 1.52, risulta $|\Lambda| = |\bigcup_{n\in\mathbb{N}} \Lambda_n| = |A|$, ove l'ultima uguaglianza vale per il Teorema 1.53. □

Osservazione 1.57. (Principio del buon ordinamento) Per il prossimo risultato ci sarà utile il cosiddetto *principio del buon ordinamento*, che si può dimostrare essere equivalente all'Assioma della Scelta. Esso afferma:
Sia A un insieme non vuoto. Allora esiste un ordinamento $\leq$ di A tale che $(A, \leq)$ è totalmente ordinato.

Teorema 1.58. *Sia Ω un campo algebricamente chiuso e sia π il suo sottocampo fondamentale. Supponiamo esista una base di trascendenza infinita B di Ω su π. Allora $|\pi(B)| = |B|$.*

Dimostrazione. Per il Teorema 1.19 sappiamo che $\pi = \mathbb{Z}_p$ oppure $\pi = \mathbb{Q}$. In ogni caso $|\pi| \leq \aleph_0$.
Sicuramente $|\pi(B)| \geq |B|$ in quanto $\pi(B) \supset B$.
Vogliamo ora dimostrare che $|\pi(B)| \leq |B|$. Per il principio del buon ordinamento possiamo ordinare B in modo che $(B, \leq)$ risulti un insieme totalmente ordinato. Osserviamo che, per argomentazioni analoghe a quelle del Teorema 1.55, basta mostrare che $|\pi[B]| \leq |B|$. Sia Ψ l'insieme dei sottoinsiemi finiti di B. Sappiamo che, preso $x \in \pi[B]$, allora esiste un sottoinsieme finito S di B tale che $x \in \pi[S]$. Inoltre, per il Teorema 1.55, se $S = \{\lambda_1, ..., \lambda_n\}$, si ha che esiste un isomorfismo $\varphi_s : \pi[S] \to \pi[x_1, ..., x_n]$, dove $x_1, ..., x_n$ sono indeterminate. Andiamo ora a considerare la mappa:

$$\begin{array}{rccc} \psi: & \pi[B] & \to & \Psi \times \bigcup_{k\in\mathbb{N}^*} \pi[x_1, ..., x_k] \\ & \pi[S] \ni p & \mapsto & (S, \varphi_s(p)) \end{array}$$

Si verifica agevolmente che questa mappa è iniettiva; quindi risulta $|\pi[B]| \leq |\Psi| \, |\bigcup_{k\in\mathbb{N}^*} \pi[x_1, ..., x_k]|$. D'altra parte, per il Teorema 1.53 e per il Lemma 1.56, si ha che $|\Psi| \, |\bigcup_{k\in\mathbb{N}^*} \pi[x_1, ..., x_k]| = |B||\pi| = |B|\aleph_0 = |B|$, ove l'ultimo passaggio vale per il Teorema 1.51, che si può applicare siccome B è infinito. □

Capitolo 2

Proprietà fondamentali

In questo capitolo tratteremo alcune "bizzarre" caratteristiche degli automorfismi del campo dei numeri complessi, che nel seguito indicheremo sempre con $\mathbb{C}$. Inoltre si parlerà di come si possono costruire (da un punto di vista teorico) questi automorfismi. Per farlo non limiteremo la trattazione a $\mathbb{C}$ ma, siccome non richiede nessuna fatica in più se non una notazione più generale, analizzaremo quest'ultimo punto per un generico campo algebricamente chiuso.

Definizione 2.1. Sia K un campo. Un *isomorfismo* tra sottocampi di K è un insieme, ϕ, di coppie ordinate di elementi di K che soddisfano le seguenti condizioni:

1. Se (a,x),(b,y) appartengono a ϕ, allora $a=b$ se e solo se $x=y$.
2. Se (a,x),(b,y) appartengono a ϕ, allora anche $(a+b,x+y)$, (ab,xy).
3. $(0,0)$ e $(1,1)$ appartengono a ϕ

L'insieme delle prime componenti delle coppie ordinate di un isomorfismo si chiama *dominio* di ϕ e l'insieme delle seconde componenti delle coppie ordinate si chiama *immagine* di ϕ.
Come al solito scriveremo che $\phi(a) = x$ se e solo se la coppia (a,x) appartiene a ϕ.

Non è difficile mostrare che dominio e immagine sono sottocampi di K; inoltre, se dominio e immagine coincidono (cioè individuano uno stesso sottocampo F di K), diremo che ϕ è un *automorfismo* di F.

Osservazione 2.2. Nei corsi di algebra, si da un'altra definizione di isomorfismo, cioè si dice che un isomorfismo di campi è una applicazione biiettiva f : $K \to F$, dove K e F sono campi, tale che:

1. *f(a+b)=f(a)+f(b)* per ogni $a, b \in K$
2. *f(ab)=f(a)f(b)* per ogni $a, b \in K$
3. $f(1_K) = 1_F$, $f(0_K) = 0_F$

Osserviamo che la definizione che abbiamo dato è equivalente a questa. Abbiamo privilegiato la prima definizione in quanto saremo interessati ad applicare il lemma di Zorn agli isomorfismi, ed esso è applicabile solamente se si ha a che fare con insiemi.

Definizione 2.3. Chiaramente la mappa identica su un sottocampo F di $\mathbb{C}$, cioè $I_F = \{(x, x)|x \in F\}$, è un automorfismo di F.
I_F è detto automorfismo *primitivo* di F. Tutti gli altri automorfismi sono chiamati *non primitivi*.

Definizione 2.4. Sia K un campo e siano ϕ e σ due isomorfismi tra sottocampi di K. Diciamo che ϕ estende σ se σ è un sottoinsieme di ϕ. Inoltre, se il dominio di ϕ è un sottocampo F di K, diciamo che ϕ estende σ a F.
N.B. Nella definizione a noi più familiare di isomorfismo, si dice che ϕ estende σ a F se $\phi_{|\text{ dominio di } \sigma} = \sigma$.

Esempio 2.5. Un esempio significativo di isomorfismo (per quanto riguarda questa trattazione) è il coniugio complesso, cioè

$$\phi = \{(a + ib, a - ib)|a, b \in \mathbb{R}\}$$

che è un automorfismo non primitivo di $\mathbb{C}$.

Teorema 2.6. *Ogni isomorfismo tra sottocampi di* $\mathbb{C}$ *estende* $I_{\mathbb{Q}}$*, l'applicazione identica su* $\mathbb{Q}$*.*

Dimostrazione. Sia ϕ un isomorfismo tra sottocampi di $\mathbb{C}$ e sia $F = \{a|\phi(a) = a\} = \{a|(a, a) \in \phi\}$. È semplice mostrare che F è un sottocampo di $\mathbb{C}$. Poichè $\mathbb{Q}$ è il sottocampo fondamentale di $\mathbb{C}$, cioè è contenuto in ogni sottocampo di $\mathbb{C}$, allora ϕ deve estendere $I_{\mathbb{Q}}$. □

Teorema 2.7. *Gli unici isomorfismi tra sottocampi di* $\mathbb{C}$ *il cui dominio include* $\mathbb{R}$ *e che mandano* $\mathbb{R}$ *in* $\mathbb{R}$ *sono* $I_{\mathbb{R}}$*,* $I_{\mathbb{C}}$ *e il coniugio complesso.*

Dimostrazione. Sia ϕ un tale isomorfismo, cioè supponiamo che $\mathbb{R}$ sia contenuto nel dominio di ϕ e che $x \in \mathbb{R}$ implichi $\phi(x) \in \mathbb{R}$. Mostriamo che ϕ preserva l'ordine in $\mathbb{R}$.
Sia $x < y$. Allora esiste $w \in \mathbb{R}^+$ tale che $y - x = w^2$. Quindi applicando ϕ (e poichè $\phi(w^2) = \phi(w)^2$) si ha che $\phi(y) - \phi(x) = \phi(w)^2 > 0$. Dunque $\phi(y) - \phi(x) > 0$, cioè $\phi(x) < \phi(y)$. Supponiamo ora per assurdo che esista $a \in \mathbb{R}$ tale che $\phi(a) \neq a$. Senza perdita di generalità sia $\phi(a) > a$. Prendiamo $q \in \mathbb{Q}$ in modo che $\phi(a) > q > a$. Per il Teorema 2.6, si ha che $\phi(q) = q$; quindi, applicando ϕ, si ha che l'ordine tra a e q si inverte, cioè risulta che $q > \phi(a)$, il che genera un assurdo.
Quindi, se $a \in \mathbb{R}$, allora si ha che $\phi(a) = a$, cioè $I_{\mathbb{R}} \subseteq \phi$.
Sia ora $\phi \neq I_{\mathbb{R}}$, cioè tale che il dominio di ϕ è un sottocampo F di $\mathbb{C}$ che contiene $\mathbb{R}$ in modo proprio. Allora si ha che $\mathbb{R} \subset F \subseteq \mathbb{C}$, con $[F : \mathbb{R}] \geq 2$. D'altra parte $[\mathbb{C} : \mathbb{R}] = 2$; dunque, per il Lemma della Torre (Lemma 1.14), vale $[F : \mathbb{R}] = 2$, ovvero il dominio di ϕ è $\mathbb{C}$. Consideriamo ora $\phi(i)$. Poichè $i^2 = -1$, si ha che $[\phi(i)]^2 = \phi(i^2) = \phi(-1) = -1$. D'altra parte le uniche radici del polinomio $x^2 = -1$ sono $\pm i$; quindi $\phi(i) = \pm i$.
Dunque, se $\phi(i) = i$, risulta $\phi = I_{\mathbb{C}}$; invece, se $\phi(i) = -i$, risulta che ϕ è il coniugio complesso. □

Osservazione 2.8. Il Teorema 2.6 implica che $\mathbb{Q}$ non ha automorfismi non banali, e il Teorema 2.7 implica lo stesso per $\mathbb{R}$. Il teorema 2.7 ha anche come

conseguenza che un qualunque automorfismo non banale di un sottocampo di $\mathbb{R}$ non può essere esteso a un automorfismo di $\mathbb{R}$.

Definizione 2.9. Un qualsiasi automorfismo di $\mathbb{C}$ diverso da $I_{\mathbb{C}}$ e dal coniugio complesso sarà nel seguito chiamato *automorfismo selvaggio* di $\mathbb{C}$.

Teorema 2.10. *Se ϕ è un automorfismo selvaggio di $\mathbb{C}$, allora ϕ fissa un sottoinsieme denso di $\mathbb{R}$, ma manda la retta reale in un sottoinsieme denso di $\mathbb{C}$.*

Dimostrazione. Per il Teorema 2.6 ϕ manda $\mathbb{Q}$ in $\mathbb{Q}$; quindi esiste un sottoinsieme denso di $\mathbb{R}$ fissato da ϕ.
Vogliamo ora far vedere che, fissato $\epsilon > 0$ e preso $z_0 = x_0 + iy_0 \in \mathbb{C}$, con $x_0, y_0 \in \mathbb{R}$, esiste un numero $l \in \mathbb{R}$ tale che $\phi(l) \in Q(z_0, \epsilon)$, dove con $Q(z_0, \epsilon)$ indichiamo il quadrato $[x_0 - \epsilon, x_0 + \epsilon] \times [y_0 - \epsilon, y_0 + \epsilon]$ nel piano complesso.
Per il Teorema 2.7 possiamo scegliere $b \in \mathbb{R}$ tale che $\phi(b) \notin \mathbb{R}$. Sia dunque $\phi(b) = c + id$, dove $c, d \in \mathbb{R}$ e $d \neq 0$.
Poniamo $S = \{\phi(rb + q) | r, q \in \mathbb{Q}\} \subset \phi(\mathbb{R})$. Dunque è sufficiente far vedere che esistono $r, q \in \mathbb{Q}$ tali che $\phi(rb + q) \in Q(z_0, \epsilon)$. Per definizione di isomorfismo e per il Teorema 2.6 si ha $\phi(rb + q) = r\phi(b) + q$ per ogni $r, q \in \mathbb{Q}$. Per densità di $\mathbb{Q}$ in $\mathbb{R}$, possiamo scegliere $r \in \mathbb{Q}$ tale che $|rd - y_0| < \epsilon$. Dunque $\phi(rb) = r\phi(b) = rc + ird$. Analogamente, possiamo prendere $q \in \mathbb{Q}$ in modo tale che $|rc + q - x_0| < \epsilon$. Quindi si ha $\phi(rb + q) = \phi(rb) + q = (rc + q) + ird = \alpha + i\beta$, dove $|\alpha - x_0| < \epsilon$ e $|\beta - y_0| < \epsilon$, cioè $\phi(rb + q) \in Q(z_0, \epsilon)$, il che completa la dimostrazione. □

Teorema 2.11. ***(Lemma di estensione)***
Sia Ω un campo algebricamente chiuso e sia ϕ un isomorfismo con dominio F e immagine K, dove F e K sono sottocampi di Ω. Preso $\alpha \in \Omega$:

1. *Se α è trascendente su F allora, preso $\beta \in \Omega$, esiste un isomorfismo che estende ϕ a $F(\alpha)$ che manda α in β se e solo se β è trascendente su K.*

2. *Se α è algebrico su F e p_α è il polinomio minimo di α su F, allora c'è una corrispondenza biunivoca*

$$\begin{array}{ccc} \{\psi : F(\alpha) \to \Omega |\ \psi_{|F} = \phi\} & \leftrightarrow & \{\beta \in \Omega |\ \beta \text{ è radice di } \phi(p_\alpha)\} \\ \psi & \mapsto & \psi(\alpha) \\ \psi : F(\phi^{-1}(\beta)) \mapsto \Omega & \hookleftarrow & \beta \\ \phi^{-1}(\beta) \mapsto \beta & & \end{array}$$

Osservazione 2.12. Il teorema sopra riportato ci dice che ogni isomorfismo con dominio F e immagine K può essere esteso a $F(\alpha)$ a meno che α sia trascendente su F e non esistano elementi trascendenti su K.

Esempio 2.13. Consideriamo $\sigma = \{(a + c\sqrt{7}, a - c\sqrt{7}) |\ a, b \in \mathbb{Q}\}$ e $\psi = \{a + b\sqrt[4]{7} + c\sqrt{7} + d\sqrt[4]{7^2}, a + ib\sqrt[4]{7} - c\sqrt{7} + id\sqrt[4]{7^2} |\ a, b, c, d \in \mathbb{Q}\}$.
Si ha che σ e ψ sono automorfismi, rispettivamente di $\mathbb{Q}(\sqrt{7})$ e di $\mathbb{Q}(i\sqrt[4]{7})$.
Infatti per il teorema sopra riportato le uniche estensioni di $I_\mathbb{Q}$ a $\mathbb{Q}(\sqrt{7})$ sono σ e la funzione identità su $\mathbb{Q}(\sqrt{7})$ in quanto $\sqrt{7}$ e $-\sqrt{7}$ sono le uniche due radici complesse del polinomio $x^2 - 7$ (e quindi σ è un isomorfismo di $\mathbb{Q}(\sqrt{7})$).
Per quanto riguarda ψ, si ha che il polinomio minimo di $\sqrt[4]{7}$ su $\mathbb{Q}(\sqrt{7})$ è $x^2 - \sqrt{7}$, che è mandato tramite σ in $x^2 + \sqrt{7}$. Le uniche due radici complesse di $x^2 + \sqrt{7}$ sono $i \pm \sqrt[4]{7}$; quindi un'estensione di σ a $\mathbb{Q}(\sqrt[4]{7})$deve mandare $\sqrt[4]{7}$ in uno di questi due numeri. Quindi ci sono solamente due possibili estensioni di σ a $\mathbb{Q}(\sqrt[4]{7})$, una delle quali è ψ.
Osserviamo che ci sono davvero tanti numeri complessi che sono trascendenti sull'immagine di ψ (cioè $\mathbb{Q}(\sqrt[4]{7})$). Quindi, per il teorema sopra riportato, per esempio, ci sono un'infinità di modi in cui estendere ψ a $\mathbb{Q}(\sqrt[4]{7}, \pi)$.

Osservazione 2.14. L'esempio sopra riportato dovrebbe convincere che ci sono molti isomorfismi tra estensioni finitamente generate di $\mathbb{Q}$. Poichè molti di questi sono automorfismi che differiscono chiaramente da $I_\mathbb{C}$ e dal coniugio complesso ne seguirà per un risultato che vedremo in seguito (cioè che un qualsiasi automorfismo tra sottocampi di $\mathbb{C}$ può essere esteso a un automorfismo di $\mathbb{C}$) che ci sono davvero tanti automorfismi di $\mathbb{C}$.

Usando l'induzione e il Lemma di estensione potremmo estendere ogni automorfismo di un sottocampo di $\mathbb{C}$ a un'estensione finitamente generata di quel sottocampo. Sfortunatamente, però, $\mathbb{C}$ non è un'estensione finitamente generata di $\mathbb{Q}$, quindi l'induzione non sarà sufficiente a provare che ogni automorfismo di un sottocampo di $\mathbb{C}$ può essere esteso a un automorfismo di $\mathbb{C}$. Per fare questo ci servirà uno strumento molto potente già usato in questa trattazione, ovvero il Lemma di Zorn.

Teorema 2.15. *Sia Ω un campo algebricamente chiuso e siano F,G sottocampi di Ω. Sia ϕ un isomorfismo con dominio F e immagine G. Allora ϕ può essere esteso a un isomorfismo con dominio $\overline{F}$ e immagine $\overline{G}$, dove con $\overline{K}$ si intende la chiusura algebrica di K.*

Dimostrazione. Sia

$$\Im = \{\theta \mid \theta \text{ è un isomorfismo che estende } \phi \text{ a un sottocampo di } \overline{F}\}$$

Vogliamo far vedere che $\Im$ soddisfa le tre ipotesi del Lemma di Zorn.

1. $\Im$ è non vuoto in quanto $\phi \in \Im$;

2. Gli isomorfismi sono insiemi di coppie ordinate, quindi tutti gli elementi di $\Im$ sono sottoinsiemi di $\Omega \times \Omega$. Sia ζ una catena contenuta in $\Im$ e sia $\sigma = \bigcup_{\theta \in \zeta} \theta$. In quanto catena, ζ è non vuota, quindi contiene almeno un isomorfismo. Da ciò ne segue che $(0,0) \in \sigma$ e che $(1,1) \in \sigma$. Siano ora (a,b),$(x,y) \in \sigma$. Allora esistono $\theta_1, \theta_2 \in \Omega$ tali che $(a,b) \in \theta_1$, $(x,y) \in \theta_2$. Siccome ζ è una catena, allora $\theta_1 \subseteq \theta_2$ oppure $\theta_2 \supseteq \theta_1$. Supponiamo per esempio che $\theta_1 \subseteq \theta_2$. Allora (a,b), $(x,y) \in \theta_2$ e quindi, siccome θ_2 è un isomorfismo, si ha che $(a+b,x+y)$, (ab,xy), $(a-b,x-y) \in \theta_2 \subseteq \sigma$. Quindi σ è un automorfismo.

3. Infine $\sigma \in \Im$, in quanto chiaramente estende ϕ. Inoltre il suo dominio è contenuto in $\overline{F}$ in quanto è unione di isomorfismi che hanno come dominio sottocampi di $\overline{F}$.

Dunque, per il lemma di Zorn, esiste un elemento massimale $\psi \in \Im$.
Supponiamo per assurdo che $\overline{F}$ non sia il dominio di σ. Allora esiste un elemento α che non appartiene al dominio di ψ. Poichè α è algebrico su F e $\overline{G}$ è algebricamente chiuso, sicuramente esiste almeno un elemento $\beta \in \overline{G}$ tale che β è zero del polinomio ottenuto applicando ψ ai coefficienti del polinomio minimo di α su F. Quindi, per il Lemma di estensione esiste almeno un'estensione di ψ a un isomorfismo appartenente a $\Im$. Questo genera un assurdo in quanto sappiamo che ψ è un elemento massimale. Quindi il dominio di ψ è $\overline{F}$.
Siccome $\overline{F}$ è un campo algebricamente chiuso e ψ è un isomorfismo, allora l'immagine di ψ è un sottocampo di $\overline{G}$ algebricamente chiuso che contiene G. Ma l'unico sottocampo di $\overline{G}$ con queste caratteristiche è $\overline{G}$ stesso. Quindi si ha che l'immagine di ψ è $\overline{G}$. □

Teorema 2.16. *Sia Ω un campo algebricamente chiuso. Ogni automorfismo di un sottocampo di Ω può essere esteso a un automorfismo di Ω.*

Dimostrazione. Sia ϕ un automorfismo di un sottocampo di Ω e sia
$\Im = \{\theta \mid \theta$ è un automorfismo che estende ϕ a un sottocampo di $\Omega\}$. La dimostrazione che $\Im$ soddisfa le tre ipotesi del Lemma di Zorn è la stessa del Teorema 2.15. Sia dunque ψ un elemento massimale di $\Im$. Sia F il dominio di ψ. Dobbiamo mostrare $F = \Omega$. Supponiamo per assurdo che ciò non sia vero, cioè che esista $\alpha \in \Omega \setminus F$. Allora:

- se α è algebrico su F, per il Teorema 2.15, possiamo estendere ψ a un automorfismo di $\overline{F}$, il che contraddice la massimalità di ψ.

- se α è trascendente su F, per il Lemma di estensione, possiamo estendere ψ a un automorfismo di $F(\alpha)$ mandando $\alpha \to \alpha$, in quanto α è anche trascendente sul codominio di ψ, che coincide con F. Questo, nuovamente, contraddice la massimalità di ψ e dunque genera un assurdo.

□

Capitolo 3

Cardinalità

In quest'ultima parte della trattazione, usando i risultati descritti nella parte preliminare su basi di trascendenza e cardinalità di insiemi, si andrà a mostrare che l'insieme degli automorfismi di $\mathbb{C}$ ha cardinalità $2^{2^{\aleph_0}}$. Più in generale si caratterizzerà la cardinalità dell'insieme degli automorfismi di un campo algebricamente chiuso Ω, facendo vedere che essa è pari a $2^{\text{card }\Omega}$.

Definizione 3.1. Sia F un campo. Un polinomio $f \in F[x]$ si dice *separabile* se tutte le radici di f sono distinte.

Definizione 3.2. Un campo F si dice *perfetto* se ogni polinomio irriducibile a coefficienti in F è separabile.

Proposizione 3.3. *Sia F un campo. Allora, se F è finito o ha caratteristica 0, è perfetto.*

Proposizione 3.4. *Sia $K \subseteq L$ un'estensione puramente trascendente. Allora ogni elemento $\alpha \in L \setminus K$ è trascendente su K.*

Dimostrazione. Si consideri $\alpha \in L$ algebrico su K e sia B una base di trascendenza di L su K tale che $L=K(B)$. Allora esiste un sottoinsieme finito di B per cui $\alpha \in K(x_1, ..., x_r)$. Quindi, per verificare che $\alpha \in K$, possiamo assumere che B sia finita, cioè $B = (x_1, ..., x_r)$. Sia ora

$$f(x) = x^n + c_1 x^{n-1} + ... + c_n \in K[x]$$

il polinomio minimo di $\alpha \in L$ su K. Possiamo supporre $\alpha \neq 0$ e quindi $c_n \neq 0$. Interpretando $K[B]$ come anello dei polinomi nelle variabili $x_1, ..., x_r$ si ha che questo è un dominio a fattorizzazione unica. Possiamo quindi scrivere $\alpha = g/h$, dove $g, h \in K[B]$ sono due elementi primi tra loro e tali che $h \neq 0$. L'equazione $f(x) = 0$ fornisce allora $(\frac{g}{h})^n + c_1(\frac{g}{h})^{n-1} + ... + c_n = 0$. Moltiplicando per h^n si ha

$$g^n + c_1 g^{n-1} h + ... + c_n h^n = 0$$

Mostriamo che h è invertibile in $K[B]$. Se così non fosse allora, preso un primo $q \in K[B]$ che divide h, per l'uguaglianza sopra riportata, dividerebbe anche g, contraddicendo il fatto che f e g sono primi tra loro. Dunque h è invertibile, ossia $h \in K^*$. In modo analogo si dimostra che $g \in K^*$ e quindi risulta che $\alpha \in K^*$. □

Lemma 3.5. *Sia Ω un campo algebricamente chiuso e sia π il suo sottocampo fondamentale. Consideriamo una base di trascendenza B di Ω su π. Allora, se $f \in \pi[x]$ è irriducibile in $\pi[x]$, f è irriducibile anche in $\pi(B)[x]$.*

Dimostrazione. Senza perdita di generalità supponiamo che f sia monico, cioè $f(x) = a_0 + a_1 x + ... + x^n \in \pi[x]$ irriducibile in $\pi[x]$. Supponiamo per assurdo che f sia riducibile in $\pi(B)[x]$. Allora esistono $g, h \in \pi(B)[x]$, $g(x) = b_0 + b_1 x + ... + x^r$, $h(x) = c_0 + c_1 x + ... + c_s x^s$, tali che $f = gh$. Sia K il campo di spezzamento di *f(x)*. Allora $f(x)$ si fattorizza in K come $f(x) = (x - \beta_1) \cdot ... \cdot (x - \beta_r) \cdot (x - \gamma_1) \cdot ... \cdot (x - \gamma_s)$, dove $\beta_1, ..., \beta_r$ sono le radici di g e $\gamma_1, ..., \gamma_s$ sono le radici di h. Allora risulta che:

- $b_0 = (-1)^r \beta_1 \cdot ... \cdot \beta_r$

  $b_i = (-1)^{r-i} \sum_{1 \leq k_1 < ... < k_{r-i} \leq r} \beta_{k_1} \cdot ... \cdot \beta_{k_{r-i}}$ per ogni *i=1,...,r-1*

- $c_0 = (-1)^s \gamma_1 \cdot ... \cdot \gamma_s$

  $c_j = (-1)^{s-j} \sum_{1 \leq k_1 < ... < k_{s-j} \leq s} \gamma_{k_1} \cdot ... \cdot \gamma_{k_{s-j}}$ per ogni *j=1,...,s-1*

Quindi per ogni $i = 0, ..., r-1$, per ogni $j = 0, ..., s-1$ si ha che b_i, c_j sono prodotto di elementi algebrici su π e dunque, per il Teorema 1.16, si ha che $b_0, ..., b_{r-1}, c_0, ..., c_{s-1}$ sono algebrici su π. Dunque, per la Proposizione 3.4, risulta che $b_0, ..., b_{r-1}, c_0, ..., c_{s-1}$ appartengono a π, ma questo è assuro in quanto avremmo una fattorizzazione non banale in $\pi[x]$. □

Teorema 3.6. *Sia Ω un campo algebricamente chiuso e sia A la famiglia degli automorfismi di Ω. Allora* card $A \geq 2^{\aleph_0}$.

Dimostrazione. Sia π il sottocampo fondamentale di Ω e sia B una base di trascendenza di Ω su π. Per prima cosa costruiamo induttivamente una successione $\{k_n\}_{n\in\mathbb{N}}$ di campi che soddisfano le seguenti proprietà:

1. $\pi(B) \subset k_1$, $k_n \subset k_{n+1}$, $[k_n : \pi(B)] < \infty$ per ogni $n \in \mathbb{N}$
2. Per ogni $n \in \mathbb{N}$ esistono 2^n $\pi(B)$-isomorfismi distinti che mandano k_n in Ω. Questi isomorfismi saranno indicati con $\phi(i_1, i_2, ..., i_n)$, dove $i_j \in \{0, 1\}$ per ogni $j = 1, ..., n$.
3. $\phi(i_1, i_2, ..., i_n, i_{n+1})$ estende $\phi(i_1, i_2, ..., i_n)$ per ogni $n \geq 2$.

Siccome π è il sottocampo fondamentale, allora $\pi = \mathbb{Z}_p$ oppure $\pi = \mathbb{Q}$. In ogni caso, per i Corollari 1.21 e 1.23 nella parte introduttiva, esistono polinomi irriducibili in $\pi[x]$ di grado arbitrariamente alto. Sia quindi f un polinomio irriducibile in $\pi[x]$ di grado ≥ 2. Poichè π è perfetto allora, per la Proposizione 3.3, f è separabile. Per il Lemma 3.5, f resta irriducibile anche in $\pi(B)[x]$. Siano a e b radici distinte di f in Ω. Notiamo che $\pi(B)(a) \cong \pi(B)[x]/(f) \cong \pi(B)(b)$. Sia $k_1 = \pi(B)(a)$. Sia $\phi(0)$ il $\pi(B)$-isomorfimo di k_1 in $\pi(B)(b)$ che manda a in b. Sia $\phi(1)$ l'isomorfismo identico di k_1.
Supponiamo ora di aver costruito i campi $k_1, k_2, ..., k_N$ che soddisfano le condizioni 1, 2 e 3. Sia $t = [k_N : \pi(B)]$. Consideriamo un polinomio irriducibile (e quindi separabile) $g \in \pi[x]$ di grado maggiore di t. Allora, sempre per il Lemma 3.5, g rimane irriducibile anche in $\pi(B)[x]$. Sia c una radice di g in Ω. Poichè c è separabile su $\pi(B)$, ne segue che c è separabile su k_N. Se

$c \in k_N$, allora risulterebbe $t < \deg g = [\pi(B)(c) : \pi(B)] \leq [k_N : \pi(B)] = t$, una contraddizione. Dunque deve essere $c \notin k_N$, cioè $[k_N(c) : k_N] \geq 2$. Sia h il polinomio minimo di c su k_N. Si ha che h è irriducibile in $k_N[x]$ e $\deg h \geq 2$. Siano $k_{N+1} = k_N(c)$ e $\phi = \phi(i_1, ..., i_N)$ uno dei 2^N isomorfismi già determinati di k_N in Ω. Poniamo $\overline{k}_N = \phi(k_N)$ e sia $\overline{h}$ il polinomio ottenuto applicando ϕ ai coefficienti di h. Chiaramente $\overline{h}$ rimane irriducibile e separabile in $\overline{k}_N[x]$, e $\deg \overline{h} = \deg h \geq 2$. Siano r_0, r_1 radici distinte di $\overline{h}$ in Ω. Quindi si ha la seguente catena di isomorfismi:

$$k_{N+1} = k_N(c) \cong k_N[x]/(h) \cong \overline{k}_N[x]/(\overline{h}) \cong \overline{k}_N(r_0) \cong \overline{k}_N(r_1)$$

Allora, per il Lemma di estensione (Lemma 2.11) ϕ può essere esteso a un isomorfismo $\phi(i_1, i_2, ..., i_N, 0)$ di k_{N+1} in $\overline{k}_N(r_0)$ mandando c in r_0. Ma, sempre per il Lemma di estensione, ϕ può anche essere esteso a un isomorfismo $\phi(i_1, i_2, ..., i_n, 1)$ di k_{N+1} in $\overline{k}_N(r_1)$ mandando c in r_1. Quindi ogni $\phi(i_1, i_2, ..., i_N)$ ha 2 estensioni distinte di isomorfismi da k_{N+1} in Ω. Dunque abbiamo trovato 2^{N+1} isomorfismi distinti di k_{N+1} in Ω. Questo completa la prova dell'esistenza della successione $\{k_n\}_{n\in\mathbb{N}}$.
Sia ora $K = \bigcup_{n=1}^{\infty} k_n$. Allora K è un campo e $\pi(B) \subset K \subset \Omega$. Sia x un numero reale con $0 < x < 1$ e sia $x = 0.i_1 i_2 ...$ l'espansione binaria di x. Sia ϕ_x la mappa definita su K da $\phi_x(t) = \phi(i_1, i_2, ..., i_n)$ se $t \in k_n$. Chiaramente ϕ_x è un $\pi(B)$-isomorfismo di K in Ω. Poichè Ω è chiusura algebrica di $\pi(B)$, possiamo applicare il Teorema 2.16 e estendere ϕ_x a un automorfismo di Ω. Dunque la mappa $x \mapsto \phi_x$ è una mappa iniettiva dall'intervallo $(0, 1)$ nell'insieme degli automorfismi di Ω. Quindi card $A \geq$ card $(0, 1) = 2^{\aleph_0}$. □

Lemma 3.7. *Sia S un insieme di cardinalità ≥ 2. Allora esiste una permutazione f di S tale che $f(x) \neq x$ per ogni $x \in S$.*

Dimostrazione. Sia

$$\mathcal{F} = \{f |\ f \text{ è una permutazione di } K,\ f(x) \neq x \text{ per ogni } x \in K,\ K \subseteq S\}$$

Se f e g sono elementi di $\mathcal{F}$, diciamo che $f < g$ se il dominio di f è contenuto nel dominio di g e g estende f. Notiamo che $\mathcal{F}$ soddisfa le ipotesi del Lemma di Zorn. Infatti:

1. $F \neq \emptyset$ in quanto, presi $a, b \in \mathcal{F}$, con $a \neq b$, e posto $K = \{a, b\}$, se consideriamo la permutazione f_K di K tale che $f_K(a) = b, f_K(b) = a$, allora $f_K \in \mathcal{F}$;

2. Sia ζ una catena di $\mathcal{F}$, $\zeta = (f_i)_{i \in \mathcal{I}}$, ove $\mathcal{I}$ è una famiglia di indici. Per ogni $i \in \mathcal{I}$ sia K_i il dominio di f_i. Definiamo $K = \bigcup_{i \in \mathcal{I}} K_i$ e $f : K \to K$ tale che $f(x) = f_i(x)$ se $x \in K_i$. Si riesce a verificare agevolmente che $f \in \zeta$ e che è un maggiorante di ζ.

Allora risulta che $\mathcal{F}$ ha un elemento massimale, che chiamiamo g. Sia A il dominio di g. Supponiamo per assurdo che $A \neq S$. Siccome g è massimale, possiamo affermare che card $(S \setminus A) = 1$. Infatti, se card $(S \setminus A) \geq 1$, presi due elementi $x, y \in A$, potremmo definire $g(x) = y,\ g(y) = x$, il che contrasta con la massimalità di g. Quindi card $(S \setminus A) = 1$, cioè $S = A \cup \{x\}, x \notin A$. Consideriamo ora un elemento $a \in A$. Sia h la mappa definita su S come segue:

- $h(a) = x$
- $h(x) = g(a)$
- $h(t) = g(t)$ se $t \in A \setminus \{a\}$

È facile federe che h è una permutazione di S e che $h(t) \neq t$ per ogni $t \in S$. Questo dà una contraddizione (in quanto g non risulterebbe un elemento massimale) e dimostra quindi che il dominio di g è S. □

Teorema 3.8. *Sia B un insieme infinito e sia A la famiglia di tutte le permutazioni di B. Allora* card $A = 2^{\text{card } B}$.

Dimostrazione. Sia $\mathcal{T}$ la famiglia di tutti i sottoinsiemi di B che hanno cardinalità maggiore o uguale a 2. Se $S \in \mathcal{T}$ allora, per il Lemma 3.7, esiste una permutazione f_S di S tale che $f_S(x) \neq x$ per ogni $x \in S$. Sia g_S la mappa definita su B da

$$g_S(x) = \begin{cases} f_S(x), & \text{se } x \in S \\ x, & \text{se } x \in B \setminus S \end{cases}$$

Allora g_S è una permutazione di B, cioè $g_S \in A$.
Sia ora h la mappa da $\mathcal{T}$ in A definita da $h(S) = g_S$ per ogni $S \in \mathcal{T}$. Facciamo vedere che h è iniettiva:
Siano $S, R \in \mathcal{T}, S \neq R$. Allora esiste $x \in (S \cup R) \setminus (S \cap R)$.

- se $x \in S$, allora $g_S(x) = f_S(x) \neq x$ e $g_R(x) = x$
- se $x \in R$, allora $g_S(x) = x$ e $g_R(x) = f_R(x) \neq x$

Quindi in ogni caso $h(S) \neq h(R)$ se $S \neq R$, cioè h è iniettiva. Ne segue che card $\mathcal{T} \leq$ card A.
Sia C la famiglia di tutti i sottoinsiemi di B. Allora C è unione disgiunta di $\mathcal{T}$ e di tutti i sottoinsiemi di B che hanno cardinalità al più 1. Dunque $2^{\text{card B}} =$ card $C = 1 +$ card $B +$ card $\mathcal{T}$. D'altra parte, siccome card $\mathcal{T} \geq$ card B, per il Teorema 1.50, vale 1+card $B +$ card $\mathcal{T} =$ card $\mathcal{T}$. Quindi

$$2^{\text{card } B} = \text{card } \mathcal{T} \leq \text{card } A.$$

Sia ora D la famiglia di tutti i sottoinsiemi di $B \times B$. Siccome $A \subset D$, e per il Teorema 1.52, abbiamo che

$$\text{card } A \leq \text{card } D = 2^{\text{card } B \times B} = 2^{\text{card } B}.$$

Quindi card $A = 2^{\text{card } B}$. □

Lemma 3.9. *Sia Ω un campo algebricamente chiuso. Allora Ω è infinito.*

Dimostrazione. Supponiamo per assurdo che Ω sia finito. Siano $\alpha_1, ..., \alpha_n$ gli elementi di Ω. Notiamo che, in quanto campo, $n \geq 2$. Allora consideriamo il polinomio $f(x) = 1 + \prod_{i=1}^{n}(x - \alpha_i)$. Allora si ha $f(\alpha_i) = 1 \neq 0$ per ogni $i = 1, ..., n$. Quindi *f(x)*, che non è costante, è privo di radici in Ω. Quindi si giunge a un assurdo, in quanto esiste un polinomio di grado ≥ 1 senza radici, il che contrasta con il fatto che Ω sia algebricamente chiuso. □

Lemma 3.10. *Siano Ω un campo algebricamente chiuso, π il suo sottocampo fondamentale, B una base di trascendenza per Ω su π. Allora, ogni permutazione σ degli elementi di B induce un automorfismo di $\pi(B)$.*

Dimostrazione. Sia $B = \{x_\lambda\}_{\lambda\in\Lambda}$, con x_λ indeterminate (o, equivalemtemente, elementi algebricamente indipendenti su π). Una permutazione di B è del tipo $x_\lambda \to x_{\sigma(\lambda)}$, ove σ è una permutazione dell'insieme della famiglia degli indici Λ. Consideriamo $a \in \pi(B)$. Allora esistono $x_{\lambda_1}, ..., x_{\lambda_n} \in B$ e $f, h \in \pi[x_{\lambda_1}, ..., x_{\lambda_n}], h \neq 0$, tali che $a = \frac{f(x_{\lambda_1},...,x_{\lambda_n})}{h(x_{\lambda_1},...,x_{\lambda_n})}$. Definiamo

$$\begin{array}{ccccc} \varphi: & \pi(B) & \to & \pi(B) \\ & a = \frac{f(x_{\lambda_1},...,x_{\lambda_n})}{h(x_{\lambda_1},...,x_{\lambda_n})} & \mapsto & \frac{f(x_{\sigma(\lambda_1)},...,x_{\sigma(\lambda_n)})}{h(x_{\sigma(\lambda_1)},...,x_{\sigma(\lambda_n)})} \end{array}$$

Si verifica agevolmente che φ è un morfismo di campi. Inoltre φ è iniettivo in quanto ogni morfismo di campi lo è. Infine, φ è suriettivo poichè ogni $c = \frac{f(x_{\lambda_1},...,x_{\lambda_n})}{h(x_{\lambda_1},...,x_{\lambda_n})}$ è immagine di $\frac{f(x_{\sigma^{-1}(\lambda_1)},...,x_{\sigma^{-1}(\lambda_n)})}{h(x_{\sigma^{-1}(\lambda_1)},...,x_{\sigma^{-1}(\lambda_n)})}$. □

Teorema 3.11. *Sia $K \subseteq F$ un'estensione di campi. Se $\mathcal{S}$ è una base di trascendenza infinita di F su K, allora ogni base di trascendenza di F su K ha la stessa cardinalità di S.*

Dimostrazione. Sia $\mathcal{T}$ una base di trascendenza di F su K. Allora, per il Teorema 1.36, $\mathcal{T}$ è infinita. Sia $s \in \mathcal{S}$. Per difinizione di base di trascendenza, s è algebrico su $K(\mathcal{T})$. Sia $f(x) \in K(\mathcal{T})[x]$ il polinomio minimo di s su $K(\mathcal{T})$. Allora esiste un sottoinsieme finito $T_s \subset \mathcal{T}$ tale che $f(x) \in K(T_s)[x]$ e, quindi, s è algebrico su $K(T_s)$.
Vogliamo ora mostrare che $\bigcup_{s\in\mathcal{S}} T_s$ è una base di trascendenza di F su K. Infatti:

- siccome $\bigcup_{s\in\mathcal{S}} T_s \subset \mathcal{T}$, allora $\bigcup_{s\in\mathcal{S}} T_s$ è algebricamente indipendente su K;
- ogni elemento di $\mathcal{S}$ è algebrico su $\bigcup_{s\in\mathcal{S}} T_s$ per definizione di T_s. Da ciò, per il Teorema 1.15, se ne ricava che $K(\bigcup_{s\in\mathcal{S}} T_s)(\mathcal{S})$ è un'estensione algebrica di $K(\bigcup_{s\in\mathcal{S}} T_s)$. In particolare, siccome $K(\mathcal{S}) \subseteq K(\bigcup_{s\in\mathcal{S}} T_s)(\mathcal{S})$, ogni elemento di $K(\mathcal{S})$ è algebrico su $K(\bigcup_{s\in\mathcal{S}} T_s)$. Inoltre $K(\mathcal{S}) \subseteq F$ è algebrica per definizione di base di trascendenza; quindi, per ciò che abbiamo detto sopra (cioè $K(\bigcup_{s\in\mathcal{S}} T_s) \subseteq K(\mathcal{S})$ è algebrica) e per la Proposizione 1.6, $K(\bigcup_{s\in\mathcal{S}} T_s) \subseteq F$ è un'estensione algebrica.

Quindi $\bigcup_{s\in\mathcal{S}} T_s$ è una base di trascendenza di F su K; inoltre, siccome $\bigcup_{s\in\mathcal{S}} T_s \subset \mathcal{T}$, allora da ciò deriva che $\bigcup_{s\in\mathcal{S}} T_s = \mathcal{T}$.
Mostriamo infine che $|\mathcal{T}| \leq |\mathcal{S}|$. Notiamo innanzitutto che gli insiemi T_s non sono necessariamente disgiunti. Per rimediare a ciò, applichiamo il principio del buon ordinamento (Osservazione 1.57) a $\mathcal{S}$. Indichiamo dunque con 1 il suo primo elemento. Definiamo $T'_1 = T_1$ e $T'_s = T_s \setminus \bigcup_{i<s} T_i$ per ogni $s \in \mathcal{S}$, $s > 1$. Notiamo che per ogni $s \in \mathcal{S}$ si ha che T'_s è finito. Inoltre, chiaramente, vale $\bigcup_{s\in\mathcal{S}} T'_s = \bigcup_{s\in\mathcal{S}} T_s$. e $T'_{s_1} \cap T'_{s_2} = \emptyset$ per $s_1 \neq s_2$. Per ogni $s \in \mathcal{S}$ fissiamo un ordinamento degli elementi di T'_s, ovvero consideriamo $T'_s = (t_1, t_2, ..., t_{k_s})$. Sia

$$\begin{array}{rccc} \phi: & \bigcup_{s\in\mathcal{S}} T'_s & \to & \mathcal{S}\times\mathbb{N}^* \\ & t_i & \mapsto & (s,i) \end{array}$$

È di facile verifica che ϕ è una mappa iniettiva. Dunque, per le osservazioni fatte sopra e per il Teorema 1.51, vale

$$|\mathcal{T}| = |\bigcup_{s\in\mathcal{S}} T_s| = |\bigcup_{s\in\mathcal{S}} T'_s| \leq |\mathcal{S}\times\mathbb{N}^*| = |\mathcal{S}|\aleph_0 = |\mathcal{S}|.$$

Invertendo il ruolo di $\mathcal{S}$ e di $\mathcal{T}$ nell'argomentazione appena esibita, si può dire che $|\mathcal{S}| \leq |\mathcal{T}|$. Dunque vale $|\mathcal{S}| = |\mathcal{T}|$. □

Teorema 3.12. *Sia Ω un campo algebricamente chiuso e sia F la famiglia di tutti gli automorfismi di Ω. Allora* card $F = 2^{\text{card }\Omega}$.

Dimostrazione. Sia A la famiglia di tutti i sottoinsiemi di $\Omega \times \Omega$. Notiamo che $F \subset A$ e che, per il Lemma 3.9, Ω è infinito. Quindi, per il Teorema 1.52, card $\Omega \times \Omega =$ card Ω. Dunque:

$$\text{card } F \leq \text{card } A = 2^{\text{card }\Omega\times\Omega} = 2^{\text{card }\Omega}.$$

Sia ora B una base di trascendenza di Ω sul suo sottocampo fondamentale π. Notiamo che per i Teoremi 1.36 e 3.11 card B è ben definita, in quanto non dipende dalla scelta della base di trascendenza. Distinguiamo due casi:

1. B è finita. Allora, per il Teorema 1.55, $\pi(B)$ è numerabile e, siccome $\pi(B) \subseteq \Omega$ è algebrica, allora per il Teorema 1.54 card $\Omega = \aleph_0$. Quindi, per il Teorema 3.6, si ha che:

$$\text{card F} \geq 2^{\aleph_0} = 2^{\text{card } \Omega}.$$

.

2. B è infinita. Allora, per il Teorema 1.58, card $\pi(B) =$ card B. Inoltre, siccome $\pi(B) \subset \Omega$ è un'estensione algebrica, per il Teorema 1.54, card $\Omega =$ card $\pi(B)$. Per il Teorema 3.8 esistono $2^{\text{card } B}$ permutazioni dell'insieme B. Ciascuna di queste, per il Lemma 3.10, induce un automorfismo distinto di $\pi(B)$. Se ϕ è uno di questi automorfismi allora, per il Teorema 2.16, ϕ può essere estesa a un automorfismo di Ω. Quindi

$$2^{\text{card } \Omega} = 2^{\text{card B}} \leq \text{card F}.$$

□

Bibliografia

[1] S. Gabelli, *Elementi di Teoria dei Campi*, 2004/2005

[2] P. Yale, *Automorphisms of the Complex Numbers*, 1966

[3] A. Charnow, *The Automorphisms of an Algebraically Closed Field*, 1970

[4] S. Bosch, *Algebra*, Springer, 2003

[5] T. Hungerford, *Algebra*, Springer, 1974

[6] J.S. Milne, *Fields and Galois Theory*, 2015

Ringraziamenti

Grazie alla mia famiglia che mi supporta costantemente negli studi.
Grazie ad Alice e a tutti i compagni di corso incontrati in questi tre anni.
Grazie alla mia relatrice Marta per la pazienza e disponibilità dimostrata.