Alma Mater Studiorum · Università di Bologna

Scuola di Scienza
Sede di Bologna

Corso di Laurea in Matematica

La Chiusura Algebrica di un Campo

Tesi di Laurea in
Matematica

Relatrice:
Marta Morigi

Presentata da:
Elisa Branchini

I Sessione
Anno Accademico 2012/2013

A mio nonno, con affetto.

Indice

Capitolo 1

Introduzione

La tesi è incentrata sulla dimostrazione dell'esistenza e unicità di una chiusura algebrica di un campo.
Enunciato fondamentale è sicuramente il lemma di Zorn (2.12), equivalente all'assioma della scelta, che afferma l'esistenza di un elemento massimale in un insieme non vuoto parzialmente ordinato. Esso è utilizzato in tutti i capitoli per dimostrare sia l'esistenza sia l'unicità di una chiusura algebrica.
Parleremo per prima di quest'ultima, trattata nel quarto e ultimo capitolo sfruttando alcune nozioni sui campi di spezzamento.
In tale capitolo dimostriamo due enunciati importanti: l'equivalenza tra una chiusura algebrica di un campo K e un campo di spezzamento su K dell'insieme S di tutti i polinomi irriducibili in $K[x]$ (teorema 4.6), e l'esistenza di un K-isomorfismo tra due campi di spezzamento di S su K (corollario 4.3). Questo ci permette di ottenere quanto voluto infatti due chiusure algebriche di K, in quanto campi di spezzamento di tutti i polinomi irriducibili a coefficienti in K, sono K-isomorfi.
Per quanto riguarda la dimostrazione dell'esistenza, invece, essa viene presentata in due capitoli, corrispondenti a due modi diversi di approcciarsi al teorema. Il primo fa riferimento principalmente a nozioni insiemistiche mentre il secondo a nozioni algebriche.
- Il primo capitolo è diviso in tre sezioni.

La prima tratta le proprietà dei numeri cardinali utili per la dimostrazione di un importante teorema (2.32) della sezione successiva, il quale afferma che se F è una estensione algebrica di un campo K allora $|F| \leq \aleph_0|K|$. Esso è fondamentale nella dimostrazione principale per controllare la cardinalità di alcuni campi.

Per la dimostrazione dell'esistenza di una chiusura algebrica prendiamo un insieme S abbastanza grande che abbia cardinalità $> \aleph_0|K|$ e consideriamo la classe Γ di tutti i campi $(E, +, \cdot)$ tali che $E \subseteq S$ e $K \subseteq E$ è una estensione algebrica. In realtà Γ è un insieme ordinato. Pertanto dimostriamo che su di esso possiamo utilizzare il lemma di Zorn; quindi esiste un elemento massimale A. Poichè A non ha estensioni di grado finito, segue che è algebricamente chiuso (proposizione 2.28). Pertanto A, essendo algebrico su K per ipotesi, è la chiusura algebrica cercata.

- La seconda dimostrazione è di tipo costruttivo in quanto costruiamo, a partire dal campo $F = E_0$, una successione di campi E_i algebrici su F nella cui unione E algebricamente chiusa risiede la chiusura algebrica di F.

Nella sezione 3.1 dimostriamo che la chiusura algebrica di F in un campo algebricamente chiuso è la chiusura algebrica di F (3.19), e grazie a ciò si ottiene quanto voluto.

Inoltre vedremo, attraverso l'uso della teria dei campi (nello specifico di quelli perfetti), che la chiusura algebrica di F è E_1 e che quindi non è necessario costruire tutta la successione.

Capitolo 2

Prima dimostrazione

2.1 I numeri cardinali

2.1.1 Conoscenze e Definizioni utili

Definizione 2.1. Un insieme *parzialmente ordinato* è un insieme non vuoto A con una relazione R, chiamata *ordine parziale di* A, che gode delle proprietà: riflessiva ($(a, a) \in R$ per ogni $a \in A$), transitiva (se $(a, b) \in R$ e $(b, c) \in R$ allora $(a, c) \in R$ per ogni $a, b, c \in A$) e antisimmetrica (se $(a, b) \in R$ e $(b, a) \in R$ allora $a = b$ per ogni $a, b \in A$).
Se $(a, b) \in R$ scriveremo $a \leq b$ (o $b \geq a$). Due elementi a e b tali che $a \leq b$ o $a \geq b$ vengono detti *comparabili*.

Definizione 2.2. Un ordine parziale su di un insieme A in cui ogni coppia di elementi è comparabile è chiamato *ordine lineare (totale o semplice)*.
Un sottoinsiene non vuoto B di A totalmente ordinato (con $\leq$) è chiamato *catena* in A.

Definizione 2.3. Sia B un sottoinsieme non vuoto di un insieme parzialmente ordinato $(A, \leq)$. Un elemento $c \in B$ è un *minimo* di B se $c \leq b$ per ogni $b \in B$, ed è un *massimo* di B se $c \geq b$ per ogni $b \in B$.
Se ogni sottoinsieme non vuoto di A ha un minimo allora A è detto *ben ordinato*.

Un *maggiorante* di un sottoinsieme B di A è un elemento $d \in A$ tale che $b \leq d$ per ogni $b \in B$.

Definizione 2.4. Sia $(A, \leq)$ un insieme parzialmente ordinato e sia m un suo elemento. Si ha che m si dice *elemento massimale di* A se per ogni $a \in A$ tale che $m \leq a$ si ha che $a = m$.

Definizione 2.5. Due insiemi A e B si dicono *equipollenti* ($A \sim B$) se esiste una mappa biettiva $A \longrightarrow B$.

Osservazione 2.6. L' equipollenza è una relazione di equivalenza sulla classe S di tutti gli insiemi.

Sia $I_0 = \emptyset$ e per ogni $n \in \mathbb{N}$ e sia $I_n = \{1, ..., n\}$. I_m e I_n sono equipollenti se e solo se $m = n$. Se un insieme A è equipollente a I_n per un qualche $n \geq 0$ A si dice *finito* e in tal caso ha esattamente n elementi, altrimenti si dice infinito.
Possiamo quindi dire che:

Definizione 2.7. Il *numero cardinale* (o la *cardinalità*) di un insieme A (denotato con $|A|$) è la classe di equivalenza di A sotto la relazione di equipollenza. $|A|$ è un cardinale finito o infinito a seconda che A sia (rispettivamente) finito o infinito.

Osservazione 2.8. La cardinalità è spesso denotata con lettere greche α, β, γ, ... 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 equipollenti, ossia $|A| = |B| \Leftrightarrow A \sim B$.

3. La cardinalitá di un insieme finito può essere identificata con il numero degli elementi dell' insieme.

Esempio 2.1 (la cardinalità di $\mathbb{N}$). Il numero cardinale di $\mathbb{N}$ è denotato abitualmente con $\aleph_0$.
Un insieme A di cardinalità $\aleph_0$ è detto *numerabile* ed ha la propietà di essere equipollente a $\mathbb{N}$. Gli insiemi $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, $\mathbb{Z}$, $\mathbb{Q}$ sono numerabili mentre $\mathbb{R}$ non lo è; dove $\mathbb{N}$ è l'insieme dei numeri naturali, $\mathbb{Z}$ l'insieme dei numeri interi, $\mathbb{Q}$ l'insieme dei numeri irrazionali e $\mathbb{R}$ l'insieme dei numeri reali.

Definizione 2.9. Siano α e β numeri cardinali. La *somma* $\alpha + \beta$ è definita come il numero cardinale $|A \cup B|$, inoltre il *prodotto* $\alpha\beta$ è il numero cardinale $|A \times B|$, dove A e B sono insiemi disgiunti tali che $|A| = \alpha$ e $|B| = \beta$.

Osservazione 2.10. Nella definizione di prodotto di elementi cardinali gli insiemi A e B possono anche non essere disgiunti.

Osservazione 2.11. Le operazioni di addizione e moltiplicazione dei numeri cardinali sono associative e commutative.

2.1.2 Sulla cardinalità

Enunciamo ora il lemma di Zorn, che è equivalente all'assiona della scelta (data una famiglia non vuota di insiemi non vuoti esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento) e quindi indipendente dagli assiomi della teoria degli insiemi.

Lemma 2.12 (Lemma di Zorn)**.** *Se A è un insieme non vuoto parzialmente ordinato in cui ogni catena in A ha un maggiorante in A allora A ha un elemento massimale.*

Mostreremo nei seguenti teoremi quale sia la cardinalità della somma o del prodotto di insiemi con diversi "numeri cardinali" .
Ad esempio nel teorema 2.15 è mostrato che la classe di tutti i numeri cardinali è lineramente ordinata (da $\leq$) e che per cardinalità finite la relazione è in accordo con l'ordinamento dei numeri non negativi.

Il fatto che non ci sia un numero cardinale più grande degli altri è conseguenza immediata del seguente:

Teorema 2.13. *Se A è un insieme e $P(A)$ è l'insieme delle sue parti allora $|A| < |P(A)|$.*

Dimostrazione. Sappiamo che esiste una mappa iniettiva $A \longrightarrow P(A)$ tale che $a \mapsto \{a\}$ quindi $|A| \leq |P(A)|$. Supponiamo che esista una mappa biettiva $f : A \to P(A)$. Allora preso $B = \{a \in A | a \notin f(a)\} \subseteq A$ esiste un $a_0 \in A$ per cui $f(a_0) = B$. Ma ciò porta ad una contraddizione infatti:
- se $a_0 \in B$ allora $a_0 \notin f(a) = B$, che è una contraddizione;
- se $a_0 \notin B$ allora $a_0 \in f(a) = B$, che è una contraddizione;
perciò $|A| \neq |P(A)|$ quindi $|A| < |P(A)|$. □

Teorema 2.14 (di Schroeder-Bernstein)**.** *Se A e B sono due insiemi tali che $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$.*

Dimostrazione. Per le ipotesi esistono due funzioni $f : A \longrightarrow B$ e
$g : B \longrightarrow A$ iniettive (che verranno usate per costruire una funzione biettiva

$h : A \longrightarrow B$). Poichè g è iniettiva, se $a \in A$ l'antimmagine $g^{\leftarrow}(a)$ può essere l'insieme vuoto (in tal caso si dice che a ha genitore vuoto in B) o $g^{\leftarrow}(a) = b$ per qualche $b \in B$. Similmente, ma scambiando A con B, avviene per f. Se continuiamo a cercare "gli antenati" degli elementi potremmo arrivare dopo un certo numero di passi ad avere un insieme vuoto (diremo che ha un "antenato vuoto") in A (o in B) oppure potremmo avere antenati all' "infinito". Possiamo quindi definire i seguenti sottoinsiemi di A e B:

$A_1 = \{a \in A | a$ ha un "antenato vuoto" in $A\}$;

$A_2 = \{a \in A | a$ ha "antenato vuoto" in $B\}$;

$A_3 = \{a \in A | a$ ha "antenati all'infinito"$\}$;

$B_1 = \{b \in B | b$ ha "antenato vuoto" in $A\}$;

$B_2 = \{b \in B | b$ ha "antenato vuoto" in $B\}$;

$B_3 = \{b \in B | b$ ha "antenati all'infinito"$\}$

Gli insiemi A_i (o B_i) sono a due a due disgiunti e la loro unione é A (o B), inoltre $f|_{A_i} : A_i \longrightarrow B_i$ con $i = 1, 3$ e $g|_{B_2} : B_2 \longrightarrow A_2$ sono biezioni. Definiamo quindi $h : A \to B$ come $h(a) = \begin{cases} f(a), & \text{per } a \in A_1 \cup A_3; \\ g^{\leftarrow}(a), & \text{per } a \in A_2. \end{cases}$
e $T : B \to A$ come $T(b) = \begin{cases} f^{\leftarrow}(b), & \text{per } b \in B_1 \cup B_3; \\ g(b), & \text{per } b \in B_2. \end{cases}$
Per $a \in A_i$ con $i = 1, 3$ si ha che $f(a) \in B_i$ e $T(h(a)) = T(f(a)) = f^{\leftarrow}(f(a)) = a$ e per $b \in B_i$ con $i = 1, 3$ si ha che $f^{\leftarrow}(b) \in A_i$ e $h(T(b)) = h(f^{\leftarrow}(b)) = f(f^{\leftarrow}(b)) = b$. Analogamente vale per $b \in B_2$ e $a \in A_2$.
Abbiamo quindi che T è l'inversa di h e di conseguenza h è una biezione. □

Teorema 2.15. *Se α e β sono numeri cardinali allora uno dei seguenti casi risulta vero:* $\alpha \leq \beta$; $\alpha \geq \beta$.
La classe dei numeri cardinali è quindi linearmente ordinata da $\leq$.

Dimostrazione. Supponiamo $|A| = \alpha$ e $|B| = \beta$. Consideriamo l'insieme F=$\{ (f, X) \mid X \subseteq A$ e $f : X \to B$ iniettiva$\}$ e la relazione definita su F: $(f_1, X_1) \leq (f_2, X_2) \Leftrightarrow X_1 \subseteq X_2$ e $f_2|X_1 = f_1$ ove $f_2|X_1$ denota la restrizione di f_2 a X_1. Abbiamo che F è non vuoto in quanto $(\emptyset, \emptyset) \in F$. Inoltre $\leq$ è un ordinamento parziale di F infatti per ogni $(f_1, X_1), (f_2, X_2), (f_3, X_3) \in F$ si

ha che:

- $(f_1, X_1) \leq (f_1, X_1)$ (banalmente)

- se $(f_1, X_1) \leq (f_2, X_2)$ (quindi $X_1 \subseteq X_2$ e $f_2|X_1 = f_1$) e $(f_2, X_2) \leq (f_1, X_1)$ (quindi $X_2 \subseteq X_1$ e $f_1|X_2 = f_2$) allora $X_1 = X_2$ e $f_1 = f_2$ ossia $(f_1, X_1) = (f_2, X_2)$

- se $(f_1, X_1) \leq (f_2, X_2)$ (quindi $X_1 \subseteq X_2$ e $f_2|X_1 = f_1$) e $(f_2, X_2) \leq (f_3, X_3)$ (quindi $X_2 \subseteq X_3$ e $f_3|X_2 = f_2$) allora $X_1 \subseteq X_2 \subseteq X_3$ e $(f_3|X_2)|X_1 = f_3|X_1 = f_2|X_1 = f_1$ quindi $X_1 \subseteq X_3$ e $f_3|X_1 = f_1$ ossia $(f_1, X_1) \leq (f_3, X_3)$.

Consideriamo una catena $C = \{(f_i, X_i) \mid i \in I\}$ di F e definiamo (f, X) nel modo seguente: $X = \bigcup_{i \in I} X_i$ e $f : X \to B$ data da $f(x) = f_i(x)$ per $x \in X_i$. Osserviamo che:

- f è ben definita: Sia $x \in X$ e supponiamo che $x \in X_k$ e $x \in X_i$ per qualche $k, i \in I$. Possiamo supporre che $(f_k, X_k) \leq (f_i, X_i)$ quindi $X_k \subseteq X_i$ e $f_i|X_k = f_k$. Pertanto $f_k(x) = f_i(x)$.

- f è iniettiva: Siano $x_1, x_2 \in X$ tali che $f(x_1) = f(x_2)$. Si ha che $x_1 \in X_j$ e $x_2 \in X_i$ per qualche $i, j \in I$ e possiamo supporre $(f_j, X_j) \leq (f_i, X_i)$ quindi $f_i|X_j = f_j$. Abbiamo quindi che $f_j(x_1) = f_i(x_1) = f_i(x_2)$ ed essendo f_i iniettiva $x_1 = x_2$.

- (f, X) è un maggiorante della catena C: ogni elemento X_i della catena è incluso in X e $f|X_i = f_i : X_i \to B$.

Quindi, per il lemma di Zorn, esiste un elemento massimale (g, X) di F. Mostriamo ora che o $X = A$ o $B =$Imm(g) (dove Imm(g) è l'immagine di g). Se entrambe queste affermazioni risultassero false esisterebbero $a \in A \backslash X$ e $b \in B \backslash$ Imm(g) e la mappa $h : X \cup \{a\} \to B$ definita da $h(x) = g(x)$ per $x \in X$ e $h(a) = b$ sarebbe iniettiva. Inoltre avremmo che $(h, X \cup a) \in F$ e $(g, X) < (h, X \cup a)$ che contraddice la massimalità di (g, X). Perciò o $X = A$ (quindi $|A| \leq |B|$) o $B =$Imm(g) (quindi $|B| \geq |A|$ (in quanto esiste $g^{-1} : B \to X \subseteq A$ iniettiva)). □

Teorema 2.16. *Ogni insieme infinito ha un sottoinsieme numerabile. In*

particolare, $\aleph_0 \leq \alpha$ *per ogni numero cardinale* α *infinito.*

Dimostrazione. Se $B \subset A$ è un sottoinsieme finito di un insieme infinito A allora $A \setminus B$ è non vuoto. Per ogni sottonsieme finito B di A scegliamo $x_B \in A \setminus B$ e consideriamo l'insieme F di tutti i sottoinsiemi finiti B di A. Definiamo quindi la mappa $f : F \to F$ nel modo seguente: $f(B) = B \cup \{x_B\}$.
Scegliamo $a \in A$ e definiamo una funzione $h : \mathbb{N} \to F$ come segue:
$\begin{cases} h(0) = \{a\} \\ h(n+1) = f(h(n)) = h(n) \cup \{x_{h(n)}\} \quad \text{per ogni } n \geq 0 \end{cases}$
Sia $g : \mathbb{N} \to A$ definita da: $\begin{cases} g(0) = a \\ g(1) = x_{h(0)} = x_{\{a\}} \\ g(n+1) = x_{h(n)} \qquad \text{per ogni } n > 1. \end{cases}$
Abbiamo quindi che $\begin{cases} g(n) \in h(n) & \text{per ogni } n \geq 0 \\ g(n) \notin h(n-1) & \text{per ogni } n \geq 1 \\ g(n) \notin h(m) & \text{per ogni } m < n. \end{cases}$
Osserviamo che g è iniettiva infatti presi n,$m \in \mathbb{N}$:
-se $n = 0$ allora $g(0) = \{a\} = g(m)$ se e solo se $m = 0$.
-se $m, n \geq 1$ con $n \neq m$ e $g(m) = g(n)$ possiamo supporre $m > n$ allora $g(m) \notin h(n) \ni g(n)$ che è una contraddizione.
Quindi $m = n$. Pertanto $|\text{Imm}(g)| = |\mathbb{N}| = \aleph_0$. □

Lemma 2.17. *Se* A *è un insieme infinito e* F *è finito allora* $|A \cup F| = |A|$. *In particolare* $\alpha + n = \alpha$ *per ogni cardinale infinito* α *e per ogni numero naturale* n.

Dimostrazione. È sufficiente supporre $A \cap F = \emptyset$. Sia $F = \{b_1, \cdots, b_n\}$ e sia $D = \{x_i \mid I \in \mathbb{N}^*\}$ un sottoinsieme numerabile di A la cui esistenza è dimostrata nel teorema 2.16 . Definiamo ora
$f : A \to A \cup F$ nel modo seguente: $f(x) = \begin{cases} b_i & \text{per } x = x_i \text{ con } 1 \leq i \leq n \\ x_{i-n} & \text{per } x = x_i \text{ con } i > n \\ x & \text{per } x \in A \setminus D \end{cases}$
Tale f è una biezione. Infatti è:
-iniettiva: notiamo che $A \setminus D, D, F$ sono insiemi disgiunti che hanno immagini disgiunte e, inoltre, $f|_{A \setminus D}$, $f|D$, $f|F$ sono iniettive quindi f è iniettiva,
-suriettiva: se $x = x_i \in D$ allora $x = f(x_{i+n})$, se $x = x_i \in F$ allora $x = f(x_i)$

e se $x \in A \setminus D$ allora $x = f(x)$.

□

Teorema 2.18. *Se α e β sono numeri cardinali tale che $\beta \leq \alpha$ e α è infinito allora $\alpha + \beta = \alpha$.*

Dimostrazione. È sufficiente dimostrare che $\alpha + \alpha = \alpha$ (infatti risulta $\alpha \leq \alpha + \beta \leq \alpha + \alpha = \alpha$). Sia A un insieme con $|A| = \alpha$ e $F = \{(f, X) \mid X \subseteq A$ e $f : X \times \{0,1\} \to X$ biezione$\}$. F è parzialmente ordinato dalla relazione: $(f_1, X_1) \leq (f_2, X_2) \Leftrightarrow X_1 \subseteq X_2$ e $f_2|_{X_1 \times \{0,1\}} = f_1$.
Prendiamo la biezione $k : \mathbb{N} \times \{0,1\} \to \mathbb{N}$ definita da $k((t,n)) = 2n + t$ con $t = 0, 1$. Per il teorema 2.16 esiste un sottoinsieme $D \subset A$ tale che $|D| = |\mathbb{N}|$. Esistono quindi una biezione tra D ed $\mathbb{N}$ ed una biezione tra $\mathbb{N} \times \{0,1\}$ e $D \times \{0,1\}$. Allora possiamo costruire una biezione $f : D \times \{0,1\} \to D$. Quindi $(f, D) \in F$ ossia F è non vuoto.
Ragionando in modo analogo alla dimostrazione del teorema 2.15, sappiamo che ogni catena ha un maggiorante e che quindi, per il lemma di Zorn, esiste un elemento massimale (g, C) di F. Prendiamo $C_0 = \{(c, 0) \mid c \in C\}$ e
$C_1 = \{(c, 1) \mid c \in C\}$. Osserviamo che C_0 e C_1 sono disgiunti. Inoltre si ha che $C_0 \cup C_1 = C \times \{0,1\}$ e quindi $|C_0| = |C_1| = |C|$. La mappa $g : C \times \{0,1\} \to C$ è una biezione quindi $|C| = |C \times \{0,1\}| = |C_0 \cup C_1| = |C_0| + |C_1| = |C| + |C|$.
Supponiamo che $|A| > |C|$. Allora, per il lemma 2.17, $A \setminus C$ è infinito. Esiste quindi, per il teorema 2.16, un sottoinsieme numerabile B di $A \setminus C$. Perciò abbiamo una biezione $\varepsilon : B \times \{0,1\} \to B$. Prendiamo
$h : (C \cup B) \times \{0,1\} \to (C \cup B)$ definita da: $h(x) = g(x)$ per ogni $x \in C \times \{0,1\}$ e $h(x) = \varepsilon(x)$ per ogni $x \in B \times \{0,1\}$. Possiamo osservare che h è una biezione (in quanto lo sono ε e g) e qiundi $(h, C \cup B) \in F$. Ma $(g, C) < (h, C \cup B)$ e ciò contraddice l'ipotesi di massimalità di (g, C) in F. Abbiamo quindi che $|C| = \alpha = |A|$ e di conseguanza $A \setminus C$ è finito. Allora, per il lemma 2.17, $|C| = |C \cup (A \setminus C)| = |A| = \alpha$. □

Teorema 2.19. *Se α e β sono numeri cardinali tali che $\beta \leq \alpha$, β è non nullo e α è infinito allora $\alpha\beta = \alpha$ e se β è finito $\beta\aleph_0 = \aleph_0$. In particolare $\alpha\aleph_0 = \alpha$.*

Dimostrazione. È sufficiente dimostrare che $\alpha\alpha = \alpha$ (infatti risulta $\alpha \leq \alpha\beta \leq \alpha\alpha = \alpha$). Prendiamo A con cardinalità α e $F = \{f : X \times X \to X \mid X$ è un sottoinsieme infinito di A e f è biettiva $\}$. F è parzialmente ordinato dalla relazione: siano $f_1 : X_1 \times X_1 \to X_1$ e $f_2 : X_2 \times X_2 \to X_2 \quad \in F$ allora $f_1 \leq f_2 \Leftrightarrow X_1 \subseteq X_2$ e $f_2|_{X_1 \times X_1} = f_1$.
Per il teorema 2.16 esiste un sottoinsieme numerabile D di A. Definiamo la mappa $g : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ nel modo seguente: $g(m, n) = 2^{m-1}(2n - 1)$.
Allora g è:
- iniettiva: se $(m, n), (t, k) \in \mathbb{N}^* \times \mathbb{N}^*$ e $2^{m-1}(2n - 1) = 2^{t-1}(2k - 1)$ allora $(2n - 1)/(2k - 1) = 2^{t-1}/2^{m-1} = 2^{t-m}$ quindi $t = m$ e $n = k$, poichè il rapporto tra due elementi dispari è dispari, e 2^{t-m} è pari.
- suriettiva: per $m = 1$ abbiamo tutti i naturali dispari, mentre per $m > 1$ al variare di n abbiamo tutti i pari.

Allora g è biettiva e quindi, essendo D numerabile, $k : D \times D \to D$ è una biezione. Allora $k \in F$ e quindi F è non vuoto.
In modo analogo alla dimostrazione del teorema 2.15, otteniamo che ogni catena ha un maggiorante e che quindi, per il lemma di Zorn, esiste un elemento massimale $g : B \times B \to B$ con $|B||B| = |B \times B| = |B|$.
Dimostreremo ora che $|B| = |A| = \alpha$.
Supponiamo che $|A \setminus B| > |B|$ allora esiste $C \subset A \setminus B$ tale che $|C| = |B| = |B \times B| = |B||B| = |C||C| = |C \times C| = |C||B| = |C \times B| = |B||C| = |B \times C|$.
Allora, per il teorema 2.18 e la definizione 2.9, $|(B \cup C) \times (B \cup C)| = |(B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C)| = |B \times B| + |B \times C| + |C \times B| + |C \times C| = (|B| + |B|) + (|C| + |C|) = |B| + |C| = |B \cup C|$ e quindi esiste una biezione $(B \cup C) \times (B \cup C) \to (B \cup C)$, che contraddice l'ipotesi di massimalità di g in F. Allora per il teorema 2.15 $|A \setminus B| \leq |B|$ e per il teorema 2.18 $|B| = |A \setminus B| + |B| = |(A \setminus B) \cup B| = |A| = \alpha$. □

Teorema 2.20. *Sia A un insieme, e per ogni $n \geq 1$ sia $A^n = A \times .... \times A$ (prodotto cartesiano di n copie di A). Allora:*

1) se A finito $|A^n| = |A|^n$; se A è infinito $|A^n| = |A|$;

2) $|\bigcup_{n\in\mathbb{N}^*} A^n| = \aleph_0|A|$

Dimostrazione. Il primo punto si dimostra per induzione qualunque sia A. Per la definizione 2.9 di prodotto di numeri cardinali se $n = 1 \quad |A^1| = |A| = |A|^1$. Supponiamo quindi che sia vero per $n-1$. Allora, per induzione, si ha che $|A^n| = |A^{n-1} \times A| = |A^{n-1}| \times |A| = |A|^{n-1}|A| = |A|^n$ e di conseguenza $|A^n| = |A|^n$ per ogni $n \in \mathbb{N}$. In particolare se A è infinito per il teorema 2.19 (in cui $\beta = \alpha = |A|$), si dimostra facilmente, per induzione su n, che $|A|^n = |A|$ per ogni $n \in \mathbb{N}$.

Il secondo punto si dimostra distinguendo due casi. Osserviamo per prima cosa che gli insiemi A^n (con $n \geq 1$) sono tra loro disgiunti.

- sia A infinito. Allora per il primo punto $|A^n| = |A|$ ed esiste quindi una mappa biettiva $f_n : A^n \to A$ per ogni valore di n. Consideriamo la funzione $f : \bigcup_{n\in\mathbb{N}^*} A^n \to \mathbb{N}^* \times A$ definita da $f(u) = (n, f_n(u))$ per $u \in A^n$. È facile vedere che tale funzione è una biezione, quindi $|\bigcup_{n\in\mathbb{N}^*} A^n| = |\mathbb{N}^* \times A| = |\mathbb{N}^*||A| = \aleph_0|A|$.

- sia A finito. Allora A è vuoto, e la cunclusione è ovvia, oppure è finito.

Nel secondo caso abbiamo $\aleph_0 = |\mathbb{N}^*| \leq |\bigcup_{n\in\mathbb{N}^*} A^n|$. D'altra parte A^n è finito ed esiste, per ogni n, una mappa iniettiva $g_n : A^n \to \mathbb{N}^*$. La mappa $g : \bigcup_{n\in\mathbb{N}^*} A^n \to \mathbb{N}^* \times \mathbb{N}^*$ definita da $g(u) = (n, g_n(u))$ per $u \in A^n$ è quindi iniettiva e, per il teorema 2.19, $|\bigcup_{n\in\mathbb{N}^*} A^n| \leq |\mathbb{N}^* \times \mathbb{N}^*| = |\mathbb{N}^*| = \aleph_0$. Perciò, per il teorema 2.14, $|\bigcup_{n\in\mathbb{N}^*} A^n| = \aleph_0$ e, per il lemma 2.17, $\aleph_0 = \aleph_0|A|$. □

2.2 Richiami di teoria dei campi

La notazione usata d'ora in poi è standard. Richiameremo di seguito alcune definizioni e teoremi basilari di teoria dei campi. Per i prerequisiti si faccia invece riferimento al libro ALGEBRA di Thomas W. Hungerford.

Definizione 2.21. Un anello K è un *campo* se è un anello commutativo unitario in cui ogni elemento non nullo ha un inverso.
Un sottoinsieme L di K è un *sottocampo* di K se è un sottoanello di K e a sua volta è un campo, ossia $1 \in L$ e se $x, y \in L$ allora $x - y \in L$ e $xy^{-1} \in L$.

Definizione 2.22. Siano L e K due campi. Se L è un sottoinsieme di K diremo che $L \subseteq K$ è una *estensione di campi*.

Definizione 2.23. Se $K \subseteq F$ è una estensione di campi allora F è un K-spazio vettoriale. Se F ha dimensione finita n come K-spazio vettoriale si dice che $K \subseteq F$ è una *estensione finita* e n si dice il *grado di F su K* (denotato con [F:K]).

Definizione 2.24. Sia $L \subseteq K$ una estensione di campi e sia $u \in K$. Si dice che u è *algebrico* su L se esiste $f \in L[x]$ tale che $f(u) = 0$. In caso contrario u si dice *trascendente*.
Inoltre K si dice *algebrico* su L se ogni elemento di K è algebrico su L.

Definizione 2.25. Sia A un anello e sia f un polinomio non costante di $A[x]$. Si dice che $a \in A$ è *radice* (o *zero*) di f se $f(a) = 0$.
Se a è radice di f in A ed f è della forma $f = (x - a)g(x) \in A[x]$ dove $g(a) \neq 0$ allora a si dice *radice semplice di f*. In caso contrario a si dice *radice multipla di f*.

Definizione 2.26. Sia $K \subseteq F$ una estensione di campi e sia u un elemento di F algebrico su K. Il polinomio monico irriducibile $f \in K[x]$ di grado $n > 0$ tale che $f(u) = 0$ si dice *polinomio minimo* di u su K e si indica con p_u.

Definizione 2.27. Un campo Ω si dice *algebricamente chiuso* se ogni polinomio in $\Omega[x]$ ha almeno una radice in Ω.

Proposizione 2.28. *Si ha che Ω è algebricamente chiuso se e solo se non ha estensioni proprie di grado finito.*

Dimostrazione. Si veda il libro "ALGEBRA" di Thomas W. Hungerford, capitolo V. □

Definizione 2.29. Un campo Ω si dice una *chiusura algebrica* di un suo sottocampo F se è algebrico su F ed è algebricamente chiuso.
Sia $F \subseteq \Omega$ una estensione di campi. L'insieme degli elementi di Ω algebrici su F è un campo e si dice *chiusura algebrica di F in Ω.*

Definizione 2.30. Cosideriamo un campo K e sia $f \in K[x]$ tale che $f \notin K$ (quindi f non è costante). Un *campo di spezzamento di f su K* è un campo E che include K tale che f si fattorizza in fattori lineari in $E[x]$ ed
$E = K(a_1, ..., a_n)$ dove $a_1, ..., a_n$ sono tutte e sole le radici di f.
Sia S un insieme di polinomi di grado positivo in $K[x]$ e sia $K \subseteq F$ una estensione di campi. Allora F si dice *campo di spezzamento su K dell'insieme S* se ogni polinomio in S si fattorizza in fattori lineari in $F[x]$ ed F è generato su K dalle radici di tutti i polinomi di S.

Teorema 2.31. *Sia f un polinomio di $F[x]$ di grado $n > 0$; allora esiste un campo di spezzamento E per f.*

Dimostrazione. Si veda nel libro "ALGEBRA" di Thomas W. Hungerford, capitolo V. □

Lemma 2.32. *Se F è una estensione algebrica di K allora $|F| \leq \aleph_0 |K|$.*

Dimostrazione. Sia T l'insieme dei polinomi monici in $K[x]$ e sia T_n l'insieme dei polinomi monici di grado n in $K[x]$ ($n \in \mathbb{N}^*$). Ogni polinomio $f \in T_n$ è del tipo $x^n + \alpha_{n-1}x^{n-1} + ... + \alpha_0$ con $n \in \mathbb{N}^*$ ed è quindi completamente individuato dai suoi n coefficienti $\alpha_{n-1}, ..., \alpha_0 \in K$. Allora per

ogni $n \in \mathbb{N}^*$ sia $f_n : T_n \longrightarrow K^n$ una biezione. Possiamo quindi dire che T_n ha la stessa cardinalità di K^n. Gli insiemi T_n e K^n sono disgiunti tra loro ossia $T_n \cap T_s = \emptyset$ e $K^n \cap K^s = \emptyset$ per ogni $n \neq s$, quindi la mappa $f : T = \bigcup_{n\in\mathbb{N}^*} T_n \longrightarrow \bigcup_{n\in\mathbb{N}^*} K^n$ definita da $f(u) = f_n(u)$ per $u \in T_n$ è ben definita e biettiva. Allora, per il teorema 2.20, $|T| = |\bigcup_{n\in\mathbb{N}^*} T_n| = |\bigcup_{n\in\mathbb{N}^*} K^n| = \aleph_0|K|$.

Ora dimostriamo che $|F| \leq |T|$.

Per ogni $f \in T$ irriducibile ordiniamo le radici di f in F e definiamo una mappa $p : F \longrightarrow T \times \mathbb{N}^*$ come segue: se $a \in F$ allora, per ipotesi, a è algebrico su K e quindi esiste ed è unico il suo polinomio minimo $f \in T$; allora ad ogni $a \in F$ associamo la coppia $(f, i) \in T \times \mathbb{N}^*$ tale che a è la i-esima radice di f. Osserviamo che $p : F \longrightarrow T \times \mathbb{N}^*$ è iniettiva. Essendo T infinito, per il teorema 2.19, $|F| \leq |T \times \mathbb{N}^*| = |T||\mathbb{N}^*| = |T|\aleph_0 = |T|$. Quindi $|F| \leq \aleph_0|K|$. □

Osservazione 2.33. Se K è infinito per il lemma precedente abbiamo che $|F| \leq \aleph_0|K| = |K|$ ma $|K| \leq |F|$ quindi $|F| = |K|$.

Proposizione 2.34. *Sia $E \subseteq F$ una estensione di campi e sia K un campo intermedio. Se K è algebrico su E ed F è algebrico su K allora F è algebrico su E.*

Dimostrazione. Si veda nel libro "ALGEBRA" di Thomas W. Hungerford, capitolo V. □

2.3 Esistenza della chiusura algebrica (prima dimostrazione)

Dimostreremo di seguito la sola esistenza della chiusura algebrica. L'unicità sarà dimostrata nel quarto capitolo.

Teorema 2.35. *Ogni campo K ha una chiusura algebrica. Se A e C sono due chiusure algebriche di K allora esiste un isomorfismo tra di essi che estende l'identità di K in sè.*

Dimostrazione. (prima dimostrazione)
Sia K un campo e scegliamo un insieme S tale che $\aleph_0|K| < |S|$. Sappiamo che $|K| \leq \aleph_0|K|$ quindi esiste una mappa iniettiva $f : K \to S$. Pertanto possiamo considerare $K \subseteq S$.
Sia Γ la classe di tutti i campi $(E, +, \cdot)$ tali che $K \subseteq E$ è una estensione algebrica e $E \subseteq S$. Le operazioni di addizione e moltiplicazione sono definite rispettivamente dalle funzioni $g : E \times E \to E$ tale che $g((a, b)) = a + b$ e $h : E \times E \to E$ tale che $h((a, b)) = ab$.
Osserviamo che le funzioni g ed h possono essere identificate con il loro grafico, che è un sottoinsieme di $E \times E \times E$. Quindi un elemento di Γ può essere identificato con un sottoinsieme di $A = S \times (S \times S \times S) \times (S \times S \times S)$. Poichè $P(A)$ è un insieme e $\Gamma \subseteq P(A)$ si ha, in particolare, che Γ è un insieme.
Inoltre Γ è diverso dall'insieme vuoto in quanto $(K, +, \cdot) \in \Gamma$.
Γ è parzialmente ordinato dalla relazione $(E_1, +_1, \cdot_1) \leq (E_2, +_2, \cdot_2)$ se e solo se $E_1 \subseteq E_2$ è una estensione di campi.
Allora ogni catena del tipo $\{(E_i, +_i, \cdot_i)\} \in \Gamma$, con $i \in I$ ha un maggiorante ossia $\bigcup E_i$.
Sia infatti, $E = \bigcup E_i$ con le operazioni definite da: se $x_1, x_2 \in E$ allora $x_1 \in E_i$ e $x_2 \in E_j$ per qualche $i, j \in I$ e possiamo supporre $E_i \subseteq E_j$ allora $x_1 + x_2 = x_1 +_j x_2$ e $x_1 x_2 = x_1 \cdot_j x_2$. Si osserva che tali operazioni sono ben definite e che E è un campo.
Sia x un elemento di E allora $x \in E_i$ per qualche $i \in I$. Essendo gli E_i

algebrici su K, per la definizione 2.24, x è algebrico su K. Quindi ogni elemento di E è algebrico su K ossia E è algebrico su K.
Allora $(E, +, \cdot)$ è un maggiorante della catena. Quindi per il lemma di Zorn esiste un elemento massimale $(A, +, \cdot)$ di Γ.
Vogliamo ora dimostrare che A è una chiusura algebrica di K. Essendo $K \subseteq A$ una estensione algebrica è sufficiente dimostrare che A è algebricamente chiuso ossia, per quanto detto nella proposizione 2.28, che non ha estensioni proprie di grado finito.
Supponiamo per assurdo che esista una estensione algebrica B di A.
Se K è infinito, per l'osservazione 2.33, $|B| = |A| = |K|$, se invece è finito per il lemma 2.32 $|A| \leq \aleph_0|K| = \aleph_0$ e quindi, per la proposizione 2.34, $|B| \leq \aleph_0|K| = \aleph_0$. In entrambi i casi $|B| < |S|$ e quindi esiste una mappa iniettiva $f : B \to S$ che estende l'identità di A in sè. Sia $B' = \text{Imm}f \subseteq S$. Allora la mappa che manda B in B' è una biezione che manda A in sè. Osserviamo che B' ha una naturale struttura di campo indotta da quella di B tramite f. Allora B' è un campo incluso in Γ, ma $A \subset B'$ e questo contraddice la massimalità di $(A, +, \cdot)$ in Γ. Ciò conclude la dimostrazione. □

Osservazione 2.36. Di fondamentale importanza per la precedente dimostrazione è la parte finale in cui si utilizza il lemma 2.32 (e quindi i teoremi sulla cardinalità ad esso correlati) per controllare la cardinalità di B. Ciò serve a dimostrare che A non ha estensioni algebriche e di conseguenza che è una chiusura algebrica del campo K.

Capitolo 3

Seconda dimostrazione

3.1 Sui campi

Definizione 3.1. Sia $F \subseteq E$ una estensione di campi. L'estensione $F \subseteq E$ si dice *finitamente generata* se esistono $a_1, ..., a_n \in E$ tale che $E = F(a_1, ..., a_n)$.

Definizione 3.2. Sia f un polinomio non costante in $F[x]$. f si dice *separabile* se nel suo campo di spezzamento non ha radici multiple.
Sia $F \subseteq E$ una estensione di campi. Un alemento $\alpha \in E$ si dice *separabile* su F se il suo polinomio minimo è separabile.
Un campo F si dice *perfetto* se ogni polinomio irriducibile $f \in F[X]$ è separabile.

Definizione 3.3. Sia 1 l'unità dell'anello A. La *caratteristica* di A è il più piccolo numero naturale $n \neq 0$ tale che $1 + 1 + ... + 1$ (n volte)$= 0$. Se non esiste tale numero n allora la caratteristica di A è *zero* per definizione.

Definizione 3.4. Siano F un campo ed f un polinomio monico irriducibile in $F[x]$. $F[\alpha]$ è *stem field* per f se $f(\alpha) = 0$.

Proposizione 3.5. *Sia $K \subseteq F$ una estensione di campi e sia u un elemento di F algebrico su K allora:*

- $K(u) \cong K[x]/(f)$ *dove* $f \in K[x]$ *è il polinomio minimo di* u*;*
- $[K(u) : K] = n > 0$ *dove* n *è il grado di* f*.*

Dimostrazione. Si veda nel libro 'ALGEBRA' di Thomas W. Hungerford, capitolo V. □

Osservazione 3.6. Se $F[\alpha]$ e $F[\beta]$ sono stem field per f allora sono isomorfi in quanto, per la proposizione 3.5, abbiamo che $F[\alpha] \cong F[x]/(f) \cong F[\beta]$.

Definizione 3.7. Sia A un anello commutativo. Un sottoinsieme (non necessariamente proprio) I di A è un *ideale* di A se è un sottogruppo di $(A, +)$ e per ogni $a \in A$ e $x \in I$ si ha che $ax \in I$.
I si dice *ideale proprio* se $I \subset A$. In particolare un ideale proprio I di A si dice *ideale massimale* se non è contenuto strettamente in nessun altro ideale proprio.

Teorema 3.8 (Lemma della torre)**.** *Siano* $K \subseteq E$ *e* $E \subseteq F$ *due estensioni di campi.* $[F : K]$ *è finito se e solo se* $[F : E]$ *e* $[E : K]$ *sono finiti. In tal caso vale* $[F : K] = [F : E][E : K]$.

Dimostrazione. Si veda il libro ALGEBRA di Thomas W. Hungerford, capitolo V. □

Proposizione 3.9. *Se* $F \subseteq E$ *è una estensione algebrica allora ogni sottoanello* R *di* E *è un campo.*

Dimostrazione. Se α è algebrico su F allora $F[\alpha]$ è un campo in quanto isomorfo a $F[X]/(f)$ dove f è il polinomio minimo di α su F. Se $\alpha \in R$ allora $F[\alpha] \subset R$ e quindi α ha un inverso in R.

□

Le dimostrazioni del teorema e delle due proposizioni seguenti sono riportate nel libro "Field and Galois Theory" di J.S.Milne (rispettivamente) nei capitoli I e II.

Teorema 3.10. *Se F è un campo allora ha caratteristica p o zero, ove p è un numero primo.*

Proposizione 3.11. *Sia F un campo e sia f un polinomio irriducibile in $F[x]$. Allora è equivalente dire:*
- tutte le radici di f sono multiple;
- F ha caratteristica $p \neq 0$ ed f è un polinomio in X^p.

Proposizione 3.12. *Ogni campo di caratteristica zero è perfetto, e ogni campo di caratteristica $p \neq 0$ è perfetto se e solo se ogni suo elemento è una p-esima potenza.*

Proposizione 3.13. *Se F è un anello commutativo con unità allora un suo ideale M è massimale se e solo se il suo anello quoziente F/M è un campo.*

Dimostrazione. Si veda il libro ALGEBRA di Thomas W. Hungerford, capitolo III. □

Teorema 3.14. *Sia A un anello e sia I un ideale di A. Allora I è proprio se e solo se non contiene l'unità di A.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che I contenga l'unità di A allora apparterrebbero all'ideale tutti i numeri ottenuti moltiplicando un qualsiasi elemento di A per 1. Pertanto risulterebbe, contro le ipotesi su I, $I = A$.
($\Longleftarrow$) I è un ideale di A non contenente l'unità di A allora $I \subset A$ ossia è un suo ideale proprio. □

Teorema 3.15. *(Teorema dell'elemento primitivo) Sia $E = F[\alpha_1, ..., \alpha_r]$ una estensione finita di F tale che $\alpha_2, ..., \alpha_r$ sono separabili su F. Allora esiste un elemento $\gamma \in E$ tale che $E = F[\gamma]$.*

Dimostrazione. Si veda il libro "Field and Galois Theory" di J.S.Milne, capitolo V. □

Proposizione 3.16. *Ogni anello commutativo ha un ideale massimale.*

Dimostrazione. Sia S l'insieme di tutti gli ideali propri in A parzialmente ordinato dalla relazione: se $I_1, I_2 \subset S$ allora $I_1 \leq I_2$ se e solo se $I_1 \subseteq I_2$. Sia $T = \{I_j\}_{j \in J}$ una catena di A e sia $K = \bigcup_{I_j \in T} I_j$. Si osservi che K è un ideale di A.
Se $1 \in K$ allora, contro l'osservazione 2.34, $1 \in I_j$ per qualche $j \in J$. Pertanto $1 \notin K$ e quindi K è un ideale proprio di A e, in particolare, è un maggiorante per T. Allora per il lemma di Zorn esiste un elemento massimale di S che è quindi un ideale massimale di A. □

Proposizione 3.17. *$K \subseteq F$ è una estensione di campi finita se e solo se F è algebrico su K e l'estensione è finitamente generata.*

Dimostrazione. Si veda il libro "Field and Galois Theory" di J.S.Milne, capitolo I. □

Proposizione 3.18. *Se Ω è algebrico su F e ogni polinomio $f \in F[x]$ si fattorizza in $\Omega[x]$ allora Ω è algebricamente chiuso.*

Dimostrazione. Sia $f = a_0 + ... + a_n x^n$ un polinomio non costante in $\Omega[x]$. Allora f ha una radice α in una estensione finita Ω' di Ω. Consideriamo le estensioni $F \subseteq E = F[a_0, ..., a_n] \subseteq L = F[a_0, ..., a_n, \alpha]$. Osserviamo che tali estensioni sono algebriche in quanto E è generato su F da elementi di Ω, algebrico su F per ipotesi, e L è generato su E da α, che è una radice di $f \in E[x]$. Allora, per la proposizione 2.34, L è algebrico su F e, in particolare, lo è anche $\alpha \in L$. Pertanto α è radice di un polinomio $g \in F[x]$ che, per ipotesi, si fattorizza in $\Omega[x]$. Allora le radici di g in Ω', e in particolare α, stanno tutte in Ω e questo conclude la dimostrazione. □

Corollario 3.19. *Sia Ω un campo algebricamente chiuso. Per ogni sottocampo F di Ω la chiusura algebrica di F in Ω è una chiusura algebrica di F.*

Dimostrazione. Se K è la chiusura algebrica di F in Ω allora, per definizione, è algebrica su F e ogni polinomio in $F[x]$ si fattorizza in essa. Quindi, per la proposizione precedente, K è una chiusura algebrica di F. □

3.2 Esistenza della chiusura algebrica (seconda dimostrazione)

Analogamente alla prima dimostrazione analizzeremo la sola esistenza della chiusura algebrica. L'unicità sarà dimostrata nel prossimo capitolo.

Dimostrazione. Consideriamo l'anello $F[..., x_f, ...]$ tale che x_f è indicizzato dai polinomi non costanti $f \in F[x]$. Sia $I \subseteq F[..., x_f, ...]$ l'ideale generato dai polinomi $f(x_f)$. Se 1 appartiene a tale ideale allora è del tipo

$$1 = g_1 f_1(x_{f_1}) + ... + g_n f_n(x_{f_n}) \tag{3.1}$$

ove $g_i \in F[..., x_f, ...]$ e $f_i \in F[x]$. Sia E una estensione di F tale che ogni f_i ha una radice $a_i \in E$ per $i = 1, ..., n$. Sia h l'omomorfismo di anelli $F[..., x_f, ...] \to F$ definito da $h(x_{f_i}) = a_i$ e $h(x_f) = 0$ per $f \notin \{f_1, ..., f_n\}$. Pertanto la relazione (3.1) diventa $h(1) = 0$, che è impossibile. Allora $1 \notin I$. Per la proposizione 3.16 abbiamo che $F[..., x_f, ...]/I$ ha un ideale massimale M/I e, in quanto tale, $I \subseteq M$. Osserviamo che $\Omega = F[..., x_f, ...]/M$, per la proposizione 3.13, è un campo. Inoltre la mappa $F \longrightarrow \Omega$ definita da $a \mapsto a + M$ è iniettiva e quindi Ω contiene una copia isomorfa di F.
Sia $f(x) = a_n x^n + ... + a_0$ un polinomio non costante in $F[x]$. Allora in $\Omega[x]$ $f(x)$ è della forma $f(\tilde{x}) = f(x + M) = a_n(x + M)^n + ... + a_0 = a_n x^n + ... + a_0 + M = f(x) + M$. Quindi $f(\tilde{x_f}) = f(x_f) + M = 0$ in quanto $f(x_f) \in I \subseteq M$. Pertanto ogni polinomio non costante in $F[x]$ ha almeno una radice in Ω.
Ripetiamo ora il procedimento partendo da $E_1 = \Omega$, anzichè da $E_0 = F$, ottenendo così il campo E_2. Procedendo ancora avremo una successione $E_0 \subseteq E_1 \subseteq E_2 \subseteq ....$.
Osserviamo che gli E_i sono algebrici su F. Infatti E_1 è generato da elementi algebrici su F e quindi è algebrico su F. Analgamente E_2 è algebrico su E_1 quindi su F e in generale ogni E_{i+1} è algebrico su E_i e quindi su F.
Sia $E = \bigcup_i E_i$ e prendiamo un polinomio non costante $g \in E[x]$. I coefficienti

di g appartengono a E_i per qualche i e quindi g ha una radice in E_{i+1}. Pertanto $E = \bigcup_i E_i$ è algebricamente chiuso. Quindi, per il corollario 3.19, la chiusura algebrica di F in E è una chiusura algebrica di F. □

Osservazione 3.20. In particolare la chiusura algebrica di F in E è E_1 in quanto algebrica su F e, per la seguente proposizione, algebricamente chiusa.

Proposizione 3.21. *Sia $F \subseteq \Omega$ una estensione di campi. Se Ω è algebrico su F e ogni polinomio non costante in $F[X]$ ha una radice in Ω allora Ω è algebricamente chiuso.*

Dimostrazione. Divideremo la dimostrazione in due casi: nel primo caso supponiamo che F sia perfetto e nel secondo caso che non lo sia.
- Supponiamo quindi che F sia perfetto. Per la proposizione 3.18 basta dimostrare che ogni polinomio irriducibile $f \in F[x]$ si fattorizza in $\Omega[x]$. Sia quindi f un polinomio irriducibile in $F[x]$ e sia E il suo campo di spezzamento. Essendo F perfetto f è separabile e quindi, per il teorema 3.15, $E = F[\gamma]$ con $\gamma \in E$. Sia $g(X)$ il polinomio minimo di γ su F allora $g(X)$ ha coefficienti in F e quindi, per ipotesi, ha una radice $\beta \in \Omega$. $F[\gamma]$ e $F[\beta]$ sono stem field per g e quindi, per l'osservazione 3.6, esiste un F-isomorfismo $F[\gamma] \to F[\beta] \subseteq \Omega$. Pertanto, come f si fattorizza su $E = F[\gamma]$, così si fattorizza su Ω.
- Supponiamo ora che F sia di caratteristica $p \neq 0$. Prendiamo quindi $F' = \{x \in \Omega \mid x^{p^m} \in F \text{ per qualche } m\}$.
Osserviamo che F' è un sottoanello di Ω in quanto chiuso rispetto a somma e prodotto. Allora, per la proposizione 3.9, F' è un campo.
Vogliamo dimostrare che (a) F' è perfetto (b) ogni polinomio in $F'[X]$ ha una radice in Ω.
(a) Sia $a \in F'$ allora $b = a^{p^m} \in F$ per qualche m. Il polimonio $X^{p^{m+1}} - b$ ha coefficienti in F e di conseguenza ha una radice $\alpha \in \Omega$. Osserviamo che $\alpha \in F'$. Ma $\alpha^{p^{m+1}} = b = a^{p^m}$ quindi $\alpha^p = a$. Allora, per la proposizione 3.12, F' è perfetto.

(b) Mostriamo dapprima che Ω è perfetto.

Sia $\alpha \in \Omega$ e sia g il suo polinomio minimo su F'. Possiamo supporre che g abbia grado $n > 0$, allora $[F'(\alpha) : F'] = n$. Supponiamo $X^p - \alpha$ irriducibile in $\Omega[X]$ e sia β una sua radice. Osserviamo che $F'(\beta, \alpha) = F'(\beta, \beta^p) = F'(\beta)$. Allora $[F'(\beta) : F'(\alpha)] = p$. Pertanto, per il teorema della torre,

$[F'(\beta) : F'] = pn$. Inoltre $g(\beta^p) = g(\alpha) = 0$ in $F(\beta)$. Allora $g(x^p)$ è un polinomio monico di grado pn con radice β e quindi è il polinomio minimo di β. In particolare $g(X^p)$ è irriducibile in $F'[X]$ ma, per la proposizione 3.11, non è separabile, il che va contro l'ipotesi che F' sia perfetto. Allora $X^p - \alpha$ non è irriducibile. Se L è un campo di spezzamento di $X^p - \alpha$ su Ω si ha che $X^P - \alpha = (X - \beta)^p$ in $L[X]$ ove $\alpha = \beta^p$. Poichè il polinomio minimo di β su Ω divide $X^p - \alpha$, è del tipo $(X - \beta)^n$ con $n < p$ ma allora, per la proposizione 3.11, $n = 1$ ossia $\beta \in \Omega$. Quindi anche Ω è perfetto.

Concludiamo ora la dimostrazione di b).

Sia $f(X) = \{\sum_i a_i X^i \mid a_i \in F'\} \in F'[X]$. Per qualche m il polinomio $\sum_i a_i^{p^m} X^i$ ha coefficienti in F e quindi una radice $\alpha \in \Omega$. Essendo Ω perfetto esiste $\beta \in \Omega$ tale che $\alpha = \beta^{p^m}$, quindi $(f(\beta))^{p^m} = (\sum_i a_i \beta^i)^{p^m} = (\sum_i a_i^{p^m} \alpha^i) = 0$. Quindi β è una radice di f.

Pertanto, ragionando come nel primo punto ma con F' al posto di F, concludiamo che Ω è algebricamente chiuso. $\square$

Capitolo 4

Unicità della chiusura algebrica

4.1 Teoremi utili

Proposizione 4.1. *Siano $\sigma : K \longrightarrow F$ un isomorfismo di campi, u un elemento di una estensione di campi di K e v un elemento di una estensione di campi di F. Se u è radice di un polinomio irriducibile $f \in K[x]$ e v una radice di $\sigma f \in F[x]$ allora σ si estende ad un isomorfismo di campi $\tilde{\sigma} : K(u) \longrightarrow F(v)$ tale che $\tilde{\sigma}(u) = v$.*

Dimostrazione. Si veda il libro ALGEBRA di Thomas W. Hungerford, capitolo V. □

Teorema 4.2. *Sia $\sigma : K \longrightarrow L$ un isomorfismo di campi e siano $S = \{f_i\}_{i \in I}$ un insieme di polinomi di grado positivo in $K[x]$ e $S' = \{\sigma(f_i)\}_{i \in I}$ il corrispondente insieme di polinomi in $L[x]$. Se F ed M sono due campi di spezzamento rispettivamente di S su K e di S' su L allora sono isomorfi.*

Dimostrazione. Supponiamo dapprima che S consista di un singolo polinomio $f \in K[x]$. Procediamo ora per induzione su $n = [F : K]$.
Se $n = 1$ allora $F = K$ ossia f si fattorizza completamente su K. Allora $\sigma(f)$ si fattorizzza su L e quindi $L = M$. Pertanto l'isomorfismo cercato è $\sigma : F = K \longrightarrow L = M$. Supponiamo quindi che l'affermazione sia vera per

$n-1$ e dimostriamola ora per n.

Sia $[F:K]=n>1$ e sia $g(x)\in K[x]$ un fattore irriducibile di f di grado maggiore di 1. Allora $\sigma(g)$ è irriducibile in $L[x]$. Siano a una radice di g in F e b una radice di $\sigma(g)$ in M. Allora, per la proposizione 4.1, esiste un isomorfismo di campi $\tau: K(a)\longrightarrow L(b)$ tale che $\tau(a)=b$; inoltre F ed M sono rispettivamente i campi di spezzamento di f su $K(a)$ e di $\sigma(f)$ su $L(b)$. Per la proposizione 3.5, $[K(a):K]$ =deg$(g)>1$ dove deg(g) è il grado di g. Quindi, per il teorema della torre, segue che $[F:K(a)]<n$. Per ipotesi induttiva, si ha quindi che τ si estende ad un isomorfismo tra F ed M.

Supponiamo ora che S sia arbitrario. Sia Δ l'insieme delle terne (E,N,τ) dove $K\subseteq E\subseteq F$, $L\subseteq N\subseteq M$ e $\tau: E\longrightarrow N$ è un isomorfismo che estende σ. Δ è un insieme parzialmente ordinato dalla relazione:

$(E_1,N_1,\tau_1)\leq(E_2,N_2,\tau_2)$ se e solo se $E_1\subseteq E_2$, $\quad N_1\subseteq N_2$ e $\tau_2|E_1=\tau_1$.

Osserviamo che $(K,L,\sigma)\in\Delta$ e quindi Δ è non vuoto. Ragionando in modo analogo alla dimostrazione del teorema 2.15, sappiamo che ogni catena ha un maggiorante e che quindi, per il lemma di Zorn, esiste un elemento massimale (F_0,M_0,τ_0) di Δ.

Supponiamo che $F_0\neq F$. Allora esiste un polinomio $f\in S$ che non si fattorizza in F_0. Pertanto, poichè F contiene tutte le radici dei polinomi in S, F contiene un campo di spezzamento F_1 di f contenente F_0. Allo stesso modo M contiene un campo di spezzamento M_1 di $\tau_0(f)=\sigma(f)$ su M_0 e possiamo quindi estendere τ_0 ad un isomorfismo $\tau_1: F_1\longrightarrow M_1$. Allora $(F_1,M_1,\tau_1)\in\Delta$ ma $(F_0,M_0,\tau_0)<(F_1,M_1,\tau_1)\in\Delta$ e ciò va contro l'ipotesi che (F_0,M_0,τ_0) sia massimale. Quindi $F_0=F$ e allo stesso modo, ma usando τ_0^{-1}, si dimostra che $M_0=M$.

Abbiamo quindi dimostrato che $\tau_0: F\longrightarrow M$ è l'estensione di σ desiderata. □

Corollario 4.3. *Sia K un campo e sia $S=\{f_i\}_{i\in I}$ un insieme di polinomi di grado positivo in $K[x]$. Se F ed M sono due campi di spezzamento di S*

su K allora sono K-isomorfi.

Dimostrazione. È sufficiente applicare il teorema 4.2 utilizzando come σ l'identità di K. □

Inoltre, dati A e B due insiemi non vuoti, il .

Proposizione 4.4. *F è una chiusura algebrica di K se e solo se $K \subseteq F$ è una estensione algebrica e per ogni estensione algebrica E di K esiste un K-monomorfismo $\phi : E \longrightarrow F$.*

Dimostrazione. ($\Longrightarrow$) Se F è una chiusura algebrica di K, $K \subseteq F$ è per definizione una estensione algebrica. Sia $K \subseteq E$ una estensione algebrica e sia $S = \{(M, \phi_M) \mid K \subseteq M \subseteq E \text{ e } \phi_M : M \longrightarrow F \text{ è un } K\text{-monomorfismo}\}$ parzialmente ordinato dalla relazione: $(M, \phi_M) \leq (N, \phi_N)$ se e solo se $M \subseteq N$ e $\phi_N | M = \phi_M$.
In modo analogo alla dimostrazione del teorema 2.15, otteniamo che ogni catena ha un maggiorante e che quindi, per il lemma di Zorn, esiste un elemento massimale $(Z, \phi_Z) \in S$.
Supponiamo $Z \neq E$ allora esiste $\alpha \in E$ tale che $\alpha \notin Z$. Osserviamo che α è algebrico su K e quindi su Z.
Sia f il polinomio minimo di α su Z, si ha che $\phi_Z(f)$ appartiene ad $F[x]$ e poichè F è algebricamente chiuso $\phi_Z(f)$ ha una radice β in F. Per la proposizione 4.1 ϕ_Z si estende ad un isomorfismo $\tilde{\phi}_Z : Z(\alpha) \longrightarrow (\phi_Z(Z))(\beta)$. In particolare $\tilde{\phi}_Z$ è un K-monomorfismo a valori in F. Allora $(Z(\alpha), \tilde{\phi}_Z) \in S$ il che contraddice la massimalità di Z. Quindi $Z = E$.
($\Longleftarrow$) Poichè l'estensione $K \subseteq F$ è algebrica si ha che F è una chiusura algebrica di K se e solo se F è algebricamente chiuso.
Sia E_1 una chiusura algebrica di F. Allora, per la proposizione 2.34, $K \subseteq E_1$ è una estensione algebrica e quindi esiste un K-monomorfismo $\Phi : E_1 \to F$. Pertanto $\Phi(E_1)$ è algebrico su K e algebricamente chiuso, in quanto isomorfo ad E_1. Inoltre, poichè F è algebrico su K, segue che $\Phi(E_1) = F$

Allora $\Phi(E_1) = F$ ossia Φ è un isomorfismo e quindi $E_1 \cong F$. Pertanto F è algebricamente chiuso. □

Proposizione 4.5. *F è una chiusura algebrica di K se e solo se $K \subseteq F$ è algebrica e per ogni estensione algebrica $K_1 \subseteq E$ e per ogni isomorfismo $\sigma : K_1 \to K$ esiste un monomorfismo $\phi : E \to F$ che estende σ.*

Dimostrazione. Tale proposizione è un caso generale della proposizione 4.4 e si dimostra in modo analogo. □

Teorema 4.6. *Sia $K \subseteq F$ una estensione di campi. Allora sono equivalenti:*
i) F è una chiusura algebrica di K;
ii) F è un campo di spezzamento su K dell'insieme S di tutti i polinomi irriducibili in $K[x]$.

Dimostrazione. (i $\Rightarrow$ ii) Sia F una chiusura algebrica di K e sia G un campo di spezzamento di S su K. Pertanto G è algebrico su K e quindi, per la proposizione 4.4, esiste un K-monomorfismo $\Phi : G \to F$. Per definizione di campo di spezzamento ogni polinomio non costante di $K[x]$ si fattorizza in $G[x]$ e quindi in $\Phi(G)[x]$. Sia $\alpha \in F$ e sia g il suo polinomio minimo in $K[x]$. Allora g è della forma $g(x) = (x-\alpha)h(x) \in F[x]$. Inoltre $g(x) = (x-a_1)^{m_1}$ $....(x-a_n)^{m_n} \in \Phi(G)[x] \subseteq F[x]$. La fattorizzazione è unica in $F[x]$ pertanto $(x-\alpha)h(x) = (x-a_1)^{m_1}.....(x-a_n)^{m_n}$ ossia esiste $i \in \{1, ..., n\}$ tale che $a_i = \alpha \in \Phi(G)$. Allora $\Phi(G) = F$ ossia Φ è un isomorfismo e quindi $G \cong F$. (ii $\Rightarrow$ i) F è campo di spezzamento di S su K quindi F è algebrico su S (e su K) e ogni elemento di S si fattorizza completamente in F. Allora, per la proposizione 3.18, F è algebricamente chiuso. Pertanto F è, per definizione, una chiusura algebrica di K. □

4.2 Dimostrazione dell'unicità della chiusura algebrica

Dimostrazione. Consideriamo l'insieme S dei polinomi irriducibili a coefficienti in K. Siano C ed A due chiusure algebriche di K. Allora, per il teorema 4.6, C ed A sono campi di spezzamento di S su K e in quanto tali, per il corollario 4.3, sono K-isomorfi.

□

Bibliografia

J.S.Milne, *Fields and Galois Theory*, 2012,

Thomas W. Hungerford, *ALGEBRA*, Springer, 2000,

Nathan Jacobson, *Theory of Field and Galois Theory*, 1994.

Capitolo 5

Ringraziamenti

Ringrazio per prima la mia relatrice Marta Morigi per la sua disponibilità e pazienza.
Ringrazio con affetto la mia famiglia e i parenti che hanno sempre creduto in me e che mi sono vicini in questo momento così importante; ma soprattutto ringrazio a mio fratello Luca che è sempre stato in silenzio durante il mio studio.
Dei ringraziamenti speciali vanno inoltre al mio ragazzo e ai miei amici più cari Gino, Crucio, Fede, Spado, Debora, Ele che mi hanno sostenuto e sopportato nei momenti più difficili dandomi affetto e gioia.