UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Matematica

Corso di Laurea in Matematica

Elaborato finale

Il Teorema dell'Elemento Primitivo

Supervisore

Alessandra Bernardi

Laureando

Giulia Biasi

Anno accademico 2015/2016

Indice

Introduzione

Il teorema dell'elemento primitivo è un importante risultato di teoria dei campi che ha notevoli conseguenze in teoria dei numeri e in teoria di Galois. Per esempio è un passo significativo per definire il gruppo di Galois.

In questo elaborato vogliamo fornire tutti i concetti necessari alla comprensione e dimostrazione del teorema, enunciarlo nella sua forma classica e dimostrarlo. Inoltre cercheremo di evidenziare alcune sue conseguenze nel contesto della teoria dei numeri.

Il teorema in questione ha come soggetto le estensioni di campi, cioè i campi ottenuti come ampliamenti di loro sottocampi. Dato un campo F si può parlare di una sua estensione E come un campo ottenuto per aggiunzione ad F di un insieme di elementi S, dunque si denota E come $F(S)$. In particolare il teorema fornisce delle ipotesi per individuare campi semplici, cioè ottenuti per aggiunzione di un singolo elemento, detto appunto elemento primitivo. È evidente che nello studio di estensioni di campi risulta vantaggioso poter individuare quando esista un elemento primitivo.

Più precisamente il teorema dell'elemento primitivo enuncia che se un'estensione E di un campo F è ottenuta per aggiunzione ad F di un numero finito di elementi separabili allora esiste un elemento α in E tale che α è separabile e $E = F(\alpha)$.

Innanzitutto ci occuperemo in dettaglio di definire il concetto di separabilità. Ora, in breve, un elemento α in un campo F è detto separabile quando lo è il suo polinomio minimo, cioè il polinomio monico in $F[x]$ di grado minimo

di cui α è radice. A sua volta un polinomio si dice separabile quando ha tutte radici distinte nel suo campo di spezzamento, vedremo che quest'ultimo è un'estensione di F con particolari caratteristiche.

All'interno di questo elaborato in un primo capitolo definiremo gli oggetti necessari alla comprensione di quanto trattato. Daremo delle basi di teoria dei campi, caratterizzando estensioni di campi e i loro elementi. Dovremo anche accennare ad alcune nozioni di teoria dei polinomi simmetrici, in quanto necessarie alla dimostrazione del teorema.

In seguito enuncieremo il teorema dell'elemento primitivo e proseguiremo con la sua dimostrazione. Nella dimostrazione tratteremo separatamente il caso in cui il campo su cui è costruita l'estensione sia infinito o finito. Nel caso di campo infinito dimostreremo per induzione, mentre sotto la seconda ipotesi procederemo direttamente. In entrambi i casi la dimostrazione riportata appoggia fortemente su tutti i concetti e i teoremi introdotti nel primo capitolo.

Infine si vuole mostrare un'esempio dell'influenza del teorema in teora dei numeri, più precisamente delle sue conseguenze sui campi di numeri, cioè le estensioni finite del campo dei numeri razionali. In quest'ultimo capitolo presenteremo nuovamente il teorema dell'elemento primitivo con delle ipotesi diverse e mostreremo come queste siano equivalenti alle ipotesi dell'enunciato classico. Anche in questo caso verranno definiti tutti i concetti necessari alla lettura di quanto scritto.

CAPITOLO 1

Nozioni preliminari e risultati utili

In questo capitolo definiremo alcuni strumenti ed enunceremo alcuni teoremi utili alla comprensione dell'enunciato del teorema dell'elemento primitivo e alla dimostrazione dello stesso.

Nella prima sezione parleremo di estensioni di campi, in particolare ne discuteremo le proprietà e ne definiremo alcune caratteristiche, tutte necessarie alla comprensione del teorema dell'elemento primitivo.

Nella seconda sezione verrà introdotto il concetto di separabilità, questo servirà a fornire le ipotesi del teorema.

Per la stesura di queste prime due sezioni sono stati consultati testi di algebra e teoria di Galois, quali [3], [2], [1] e [4].

Infine nella terza sezione accenneremo ad alcuni concetti della teoria dei polinomi simmetrici, quali la definizione dei polinomi simmetrici elementari e il teorema di Newton, a volte detto il Teorema Fondamentale Dei Polinomi Simmetrici. Questi saranno necessari a giustificare alcuni passaggi della dimostrazione del teorema dell'elemento primitivo. Per eventuali approfondimenti a questa sezione si fa riferimento a [3, chapter 2].

1.1 Estensioni di Campi

Iniziamo col definire alcuni oggetti fondamentali per la comprensione del teorema dell'elemento primitivo, per la stesura di questa sezione si è fatto riferimento in particolare a [2], [1] e [3].

Il teorema dell'elemento primitivo prende in considerazione estensioni di campi, vediamo come queste sono definite.

Definizione 1.1. (Estensione di Campi) Siano E e F campi tali che $E \subset F$, allora E è detto estensione di F e lo si denota con $E|F$.

Esempio 1.1.1. Consideriamo i campi $\mathbb{R}$ e $\mathbb{Q}$, poichè $\mathbb{Q} \subset \mathbb{R}$, allora $\mathbb{R}$ è un'estensione di $\mathbb{Q}$.

Considerato anche $\mathbb{C}$ e osservato che $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, possiamo dire che $\mathbb{C}$ è estensione di $\mathbb{R}$ e $\mathbb{Q}$.

Proprietà importante di un campo è la sua caratteristica, la definiamo.

Definizione 1.2. (Caratteristica di un Campo) Sia F un campo, questo si dice avere caratteristica n, denotata come $\mathrm{ch}(F) = n$, se n è il minimo intero positivo per il quale si ha

$$n \cdot 1 = 0. \tag{1.1}$$

Se non esiste n che soddisfi (1.1), allora si dice che F ha caratteristica 0, $\mathrm{ch}(F) = 0$.

Esempio 1.1.2. I campi $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ hanno tutti caratteristica zero,

$$\mathrm{ch}(\mathbb{Q}) = \mathrm{ch}(\mathbb{R}) = \mathrm{ch}(\mathbb{C}) = 0.$$

Il campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ha caratteristica p, $\mathrm{ch}(\mathbb{F}_p) = p$.

Possiamo costruire estensioni di campi partendo da un campo e aggiungendo ad esso altri elementi. Definiamo questo procedimento.

Definizione 1.3. (Aggiunzione) Siano $E|F$ un'estensione di campi e $A \subset E$ sottoinsieme. Indichiamo con $F(A)$ il più piccolo sottocampo di E contente F e A, diciamo che $F(A)$ è ottenuto da F per aggiunzione di A.

Notiamo che $F(A)$ può essere anche detta detta l'estensione di F generata da A.

Osserviamo inoltre che evidentemente $F(A)$ è a sua volta un'estensione del campo F.

Osservazione 1. Siano $E|F$ estensione di campi e $\alpha_1, \ldots, \alpha_n \in E$, allora

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r, \ldots, \alpha_n)$$

per ogni r tale che $0 \leqslant r \leqslant n$.

Dimostrazione. [3, Corollary 4.1.11, page 77] □

Esempio 1.1.3. Considerati $\mathbb{R}$ estensione del campo $\mathbb{Q}$ e $\sqrt{2}, \sqrt{3} \in \mathbb{R}$, grazie all'Osservazione 1, possiamo affermare che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$.

In particolare

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

cioè otteniamo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ per aggiunzione, prima di $\sqrt{2}$ a $\mathbb{Q}$, poi di $\sqrt{3}$ a $\mathbb{Q}(\sqrt{2})$.

Data un'estensione di campi $E|F$, si può osservare che E è uno spazio vettoriale su F, non lo dimostriamo in quanto immediato. Ciò ci permette di definire il grado di un'estensione di campi.

Definizione 1.4. (Grado di un'estensione di campi) Sia $E|F$ un'estensione di campi, definiamo il grado di E su F come la dimensione su F di E visto come spazio vettoriale su F, lo denotiamo come

$$[E : F] := \dim_F(E).$$

Esempio 1.1.4. Abbiamo visto nell'Esempio 1.1.1 che $\mathbb{C}$ è un'estensione del campo $\mathbb{R}$, in particolare $[\mathbb{C} : \mathbb{R}] = 2$. Infatti possiamo osservare che $\mathbb{C}$ è uno spazio vettoriale sul campo $\mathbb{R}$ con base $\{1, i\}$.

Introduciamo ora la distinzione tra gli elementi algebrici e non algebrici (trascendenti) di un'estensione di campi $E|F$, in particolare definiamo gli elementi algebrici.

Definizione 1.5. (Elemento Algebrico) Siano $L|F$ un'estensione di campi e $\alpha \in L$. Un elemento α si dice algebrico su F se esiste un polinomio $f \in F[x]$ non nullo tale che $f(\alpha) = 0$.

Un elemento non algebrico è anche detto trascendente.

Esempio 1.1.5. (i) Possiamo considerare $\sqrt{2} \in \mathbb{R}$, questo è algebrico su $\mathbb{Q}$ in quanto radice del polinomio $x^2 - 2 \in \mathbb{Q}[x]$.

(ii) Possiamo mostrare che $\sqrt{2} + \sqrt{3}$ è algebrico su $\mathbb{Q}$. Consideriamo il polinomio

$$(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

Svolgendo otteniamo $x^4 - 10x^2 + 1$, cioè $\sqrt{2} + \sqrt{3}$ è radice di un polinomio non costante in $\mathbb{Q}[x]$.

Con queste nozioni possiamo ora caratterizzare varie estensioni. Daremo cioè la definizione di estensione finita, algebrica e semplice.

In particolare il teorema dell'elemento primitivo ci fornirà le ipotesi necessarie ad individuare quando un'estensione finita di campi possa essere detta semplice.

Definizione 1.6. (Estensione Finita) Sia $E|F$ un'estensione di campi, questa è detta finita se $[E : F] < \infty$.

Esempio 1.1.6. Come visto negli esempi precedenti, $\mathbb{C}|\mathbb{R}$ è un'estensione finita.

Definizione 1.7. (Estensione Algebrica) Sia $E|F$ un'estensione di campi, questa è detta algebrica se ogni elemento $\alpha \in E$ è algebrico su F, o alteravivamente se non esistono in E elementi trascendenti su F.

Definizione 1.8. (Estensione Semplice) Sia $E|F$ un'estensione di campi, questa è detta estensione semplice se esiste un elemeno $b \in E$ tale che $E = F(b)$.

Esempio 1.1.7. Consideriamo $\mathbb{C}$ estensione del campo $\mathbb{R}$ e $i \in \mathbb{C}$, poichè

$$\mathbb{C} = \mathbb{R}(i),$$

allora possiamo affermare che $\mathbb{C}$ è un'estensione semplice di $\mathbb{R}$.

Ci tornerà utile la seguente proposizione, caratterizzante le estensioni finite.

Proposizione 1.1.1. *Ogni estensione di campi finita è algebrica.*

Dimostrazione. Si rimanda a [3, p. 93]. □

Introduciamo ora chiusure algebriche e campi algebricamente chiusi: ci serviranno per fare delle osservazioni sul teorema dell'elemento primitivo nel contesto dei campi di numeri, che definiremo nel Capitolo 3. Definiamo i seguenti oggetti come in [7, Par. 5.1.] e [3, Sect. 4.4.].

Definizione 1.9. (Chiusura Algebrica di F in E) Sia $E|F$ estensione di campi, il campo $\overline{F_K}$ degli elementi di E algebrici su F è detta la chiusura algebrica di F in E.

Il campo F è detto algebricamente chiuso in E se ogni $\alpha \in E$ elemento algebrico su F sta a sua volta in F, cioè se $F = \overline{F_K}$.

Definizione 1.10. (Campo Algebricamente Chiuso) Sia F un campo, questo si dice algebricamente chiuso se è algebricamente chiuso su ognuna delle sue estensioni.

Definizione 1.11. (Chiusura Algebrica) Sia F un campo, definiamo la chiusura algebrica di F il campo denotato come $\overline{F}$, unico a meno di isomorfismo, tale che $\overline{F}$ sia algebrico su F e algebricamente chiuso.

Esempio 1.1.8. Consideriamo ancora le estensioni di campi $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Ora, $\mathbb{C}|\mathbb{Q}$ e $\mathbb{R}|\mathbb{Q}$ non sono algebriche, esistono infatti elementi trascendenti.

L'estensione $\mathbb{C}|\mathbb{R}$ invece è algebrica e finita, in particolare $\mathbb{C}$ è la chisura algebrica di $\mathbb{R}$.

1.2 Campo di Spezzamento e Separabilità

Il teorema dell'elemento primitivo fornirà delle ipotesi su un'estensione di campi che ne assicurino la semplicità, per comprendre queste ipotesi occorre introdurre il concetto di separabilità. Quest'ultimo è legato strettamente alla nozione di campo di spezzamento di un polinomio, iniziamo dunque con questa definizione.

Definizione 1.12. (Campo di Spezzamento)
Dato F campo qualsiasi e $p(x) \in F[x]$ un polinomio, L è detto campo di spezzamento di $p(x)$ se é un'estensione del campo F tale che

- $L = F(\gamma_1, \gamma_2, ..., \gamma_n)$ con γ_i in numero finito che siano radici di p,

- $p(x)$ si spezza interamente nel prodotto di fattori di primo grado, quando visto come polinomio a coefficienti in L,

- L è il più piccolo campo in cui vale ciò.

Esempio 1.2.1. Consideriamo il polinomio $f(x) = x^2 + 1 \in \mathbb{R}[x]$, un suo campo di spezzamento su $\mathbb{R}$ è $\mathbb{C} = \mathbb{R}(i)$.

Lo stesso polinomio f avrà campi di spezzamento diversi su campi diversi, ad esempio f su $\mathbb{Q}$ ha campo di spezzamento $\mathbb{Q}(i)$, mentre un campo di spezzamento di f su $\mathbb{C}$ è proprio $\mathbb{C}$ stesso.

Introduciamo ora il concetto di separabilità di un polinomio e, conseguentemente, di un elemento in un'estensione di campi

Definizione 1.13. (Polinomio Separabile) Sia F un campo, allora un polinomio $p(x) \in F[x]$ è detto separabile se ha tutte radici distinte nel suo campo di spezzamento.

Esempio 1.2.2. Dato un campo K, posso individuare quando un polinomio monico non costante sia separabile su K grazie al Teorema 1.4.2..

Ad esempio, per ogni $n > 0$, un polinomio $f(x) \in \mathbb{Q}[x]$ della forma $f(x) := x^n - 1$ è separabile su $\mathbb{Q}$, infatti $f'(x) = nx^{n-1}$ e dunque f e f' sono coprimi.

Per arrivare alla definizione di elemento separabile in un'estensione di campi occorre prima definire il polinomio minimo dell'elemento.

Definizione 1.14. (Polinomio Minimo) Siano $L|F$ un'estensione di campi e $\alpha \in L$ elemento algebrico su F. Il polinomio minimo di α su F è l'unico polinomio $f \in F[x]$ tale che

- f è monico,

- $f(\alpha) = 0$,

- f è il polinomio di grado minimo fra tutti i polinomi $g \in F[x]$ non nulli tali che $g(\alpha) = 0$.

Possiamo caratterizzare ulteriormente il polinomio minimo di un elemento algebrico tramite la seguente proposizione.

Proposizione 1.2.1. *Siano $E|F$ un'estensione di campi, $\alpha \in E$ elemento algebrico su F e $p \in F[x]$ il polinomio minimo di α. Sia dunque $f \in F[x]$ un polinomio monico non costante, sono equivalenti:*

(i) $f = p$ (cioè f è proprio il polinomio minimo di α su F),

(ii) f è il polinomio di grado minimo tale che $f(\alpha) = 0$,

(iii) f è irriducibile su F e $f(\alpha) = 0$.

Dimostrazione. Si fa riferimento a [3, Proposition 4.1.5, p. 75] □

Esempio 1.2.3. (i) Il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2 - 2$, ciò segue dall'irrazionalità di $\sqrt{2}$, la quale suggerisce che $\sqrt{2}$ non possa essere radice di polinomi di grado 1 in $\mathbb{Q}$.

(ii) Riprendendo l'Esempio 1.1.5 osserviamo che $x^4 - 10x^2 + 1$ è proprio il polinomio minimo di $\sqrt{2} + \sqrt{3}$ in $\mathbb{Q}$. (dimostrazione [3, Example 4.1.7.])

Possiamo ora definire la separabilità di un dato elemento.

Definizione 1.15. (Elemento Separabile) Sia F un campo, un elemento $\alpha \in F$ è detto separabile quando lo è il suo polinomio minimo.

Esempio 1.2.4. Consideriamo il campo $\mathbb{Q}$ e il polinomio irriducibile $p(x) \in \mathbb{Q}[x]$ definito come

$$p(x) := x^2 - 1 = (x - \sqrt{2})(x + \sqrt{2}).$$

Osserviamo che $p(x)$ ha radici $\sqrt{2}, -\sqrt{2}$ e che $\mathrm{ch}(\mathbb{Q}) = 0$. Ora, sapendo che in un campo K, tale che $\mathrm{ch}(K) = 0$, ogni polinomio irriducibile $q(x) \in K[x]$ è separabile (ce lo assicura la Proposizione 5.33 [7, p. 192]), allora possiamo affermare che $p(x)$ è separabile. Abbiamo già visto nell'Esempio 1.2.3 che $p(x)$ è il polinomio minimo di $\sqrt{2}$, possiamo quindi concludere che anche $\sqrt{2}$ è separabile.

Nelle dimostrazioni a seguire saranno necessari alcuni teoremi sulla separabilità dei polinomi.

In particolare il Teorema 1.2.2 ci presenta una definizione equivalente di polinomio separabile sotto alcune ipotesi, mentre il Teorema 1.2.3 ci assicura la separabilità di polinomi entro certe condizioni.

Teorema 1.2.2. *Sia $f \in K[x]$ un polinomio monico non costante*

$$f \text{ separabile} \Leftrightarrow (f, f') = 1.$$

Dimostrazione. Vediamo dapprima l'implicazione $\Rightarrow$.

Sia f separabile con α radice in un estensione di K

$$\Rightarrow f = (x - \alpha)h, \text{ con } h(\alpha) \neq 0$$

$$\Rightarrow f' = h + (x - \alpha)h'$$

$f'(\alpha) = h(\alpha) \neq 0$ cioè α non è radice di f', quindi f e f' non hanno radici in comune, e dunque non hanno nemmeno fattori in comune

$$\Rightarrow (f, f') = 1.$$

Dimostriamo ora l'implicazione $\Leftarrow$.

Abbiamo $(f, f') = 1$ cioè le radici di f non sono radici di f', dunque ogni radice di f non è multipla e quindi f è separabile. □

Teorema 1.2.3. *Dato un campo K di caratteristica* $\mathrm{ch}(K) = 0$ *si ha che:*

$$f \in K[x] \text{ irriducibile} \Rightarrow f \text{ separabile.}$$

Dimostrazione. Sia f irriducibile in $K[x]$. Per il Teorema 1.4.2 si ha che:

$$(f, f') \neq 1 \Leftrightarrow f' = 0.$$

Infatti se $(f, f') \neq 1$ allora $f | f'$ perchè f è irriducibile, ma ciò è vero se e solo se $f' = 0$ in quanto $\deg(f') < \deg(f)$.

Dunque $(f, f') = 1$ (f separabile) se e solo se $f' = 0$. Poichè $\mathrm{ch}(K) = 0$ ed f è irriducibile allora f non è costante e quindi $f' \neq 0$. □

1.3 Polinomi Simmetrici e Teorema di Newton

Nella dimostrazione del teorema dell'elemento primitivo, nel caso di F campo infinito (Capitolo 2, Sezione 2), dovremo appoggiarci in parte alla teoria dei polinomi simmetrici per poter giustificare alcuni passaggi.

In questa sezione sono introdotti i concetti necessari alla comprensione della suddetta dimostrazione, quali la nozione di polinomio simmetrico elementare, il

Teorema Fondamentale dei Polinomi Simmetrici, anche detto teorema di Newton, ed un suo corollario. Si fa riferimento per approfondimenti e dimostrazioni a [3, Chapter 2].

Definizione 1.16. (Polinomi Simmetrici Elementari) Siano F un campo e $x_1, x_2, ..., x_n$ variabili di polinomi a coefficienti in F. Definisco i σ_i polinomi simmetrici elementari di $x_1, x_2, ..., x_n$ come segue:

$$\sigma_1 := \sum_{i=1}^{n} x_i, \ , \ . \ . \ . \ , \sigma_r := \sum_{i_1<...<i_r} x_{i_1} \cdots x_{i_r}, \ . \ . \ . \ , \sigma_n := \prod_{i=1}^{n} x_i.$$

Esempio 1.3.1. Sia F un campo qualsiasi, definiamo esplicitamente i polinomi simmetrici elementari delle variabili x_1, x_2, x_3, x_4.

Chiamiamo $\sigma_i(x_1, x_2, x_3, x_4) = \sigma_i$, dunque

$$\sigma_1 := \sum_{i=1}^{4} x_i = x_1 + x_2 + x_3 + x_4,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$$

$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,$$

$$\sigma_4 = x_1x_2x_3x_4.$$

Teorema 1.3.1. *(Newton) Ogni polinomio simmetrico in $F[x_1, ..., x_n]$ può essere scritto in modo unico come un polinomio nei polinomi simmetrici elementari di $x_1, ..., x_n$ a coefficienti in F.*

Corollario 1.3.2. *Dati $F \subset L$ estensione di campi, $f \in F[x]$ e $\gamma_1, \gamma_2, ..., \gamma_n \in L$ radici di f allora ogni polinomio simmetrico a coefficienti in F calcolato su $\gamma_1, \gamma_2, ..., \gamma_n$ assume valori in F.*

CAPITOLO 2

Teorema Classico

Il seguente capitolo è strutturato in tre sezioni: nella prima è enunciato il Teorema dell'elemento primitivo nella sua forma classica, nella seconda il teorema è dimostrato sotto l'ipotesi di campo infinito, infine nella terza sezione è dimostrato il teorema nel caso di campo finito, con ciò si completa la dimostrazione del teorema classico.

La dimostrazione presentata è frutto di una rielaborazione partita da [3], in particolare dalla dimostrazione in [3, Theorem 5.4.1, p. 119]. Più precisamente in alcuni passaggi della dimostrazione del punto (2.5) si fa riferimento a [3, Chapter 2], come visto nella Sezione 1.3, mentre per qualche chiarificazione si è consultato [7].

2.1 Il Teorema Dell'Elemento Primitivo - enunciato classico

Teorema 2.1.1. *Sia* $L = F(\alpha_1, ..., \alpha_n)$ *estensione di campi finita, con* α_i *separabili su* F*, allora esiste un elemento* $\alpha \in L$ *tale che*

- α *è separabile su* F *e*
- $F(\alpha) = L$.

Inoltre, se F è un campo infinito, esistono $t_1, ..., t_n \in F$ tali che

$$\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n.$$

2.2 Dimostrazione su F campo infinito

Supponiamo inizialmente che F sia un campo infinito e che il campo $L := F(\alpha_1, ..., \alpha_n)$ sia una sua estensione finita tale che α_i sia separabile per ogni $i \in \{1, \ldots, n\}$, procederemo a dimostrare il teorema per induzione su n.

$n = 1$ In questo caso non c'è nulla da dimostrare.

$n = 2$ Abbiamo dunque $L = F(\beta, \gamma)$ con β e γ separabili. Consideriamo $f, g \in F[x]$ tali che

- f sia il polinomio minimo di β, e siano $l := \deg(f)$ e $\beta_1 := \beta, \beta_2, ..., \beta_l$ le sue radici (queste sono distinte),
- g sia il polinomio minimo di γ, e siano $m := \deg(g)$ e $\gamma_1 := \gamma, \gamma_2, ..., \gamma_m$ le sue radici (queste sono distinte).

F è infinito, quindi esiste $\lambda \in F$ tale che

$$\lambda \neq \frac{\beta_1 - \beta_r}{\gamma_s - \gamma_j} \text{ per } i \neq r,\ 1 \leq i, r \leq s \text{ e per } j \neq s,\ 1 \leq j, s \leq m$$

$$\Rightarrow \lambda(\gamma_s - \gamma_j) \neq \beta_i - \beta_r \Rightarrow \lambda\gamma_s - \lambda\gamma_j \neq \beta_i - \beta_r$$

$$\Rightarrow \lambda\gamma_s + \beta_r \neq \lambda\gamma_j + \beta_i \tag{2.1}$$

$$\Rightarrow \beta_i \neq \beta_r + \lambda\gamma_s - \lambda\gamma_j. \tag{2.2}$$

Dunque posti $r = s = 1$, vale $\forall i \in \{2, ..., l\}$, $\forall j \in \{2, ..., m\}$

$$\beta_i \neq \beta + \lambda\gamma - \lambda\gamma_j. \tag{2.3}$$

Fissato questo $\lambda \in F$ vogliamo innanzitutto mostrare che

$$F(\beta + \lambda\gamma) = F(\beta, \gamma), \tag{2.4}$$

infatti vedremo in seguito che $\beta + \lambda\gamma$ è separabile sul campo F, cioè è proprio dell'elemento primitivo che stiamo cercando.

Dimostriamo dunque le due inclusioni di (2.4).

- $F(\beta+\gamma) \subset F(\beta,\gamma)$: ovvio in quanto $\lambda \in F \subset F(\beta,\gamma)$, $\beta+\lambda\gamma \in F(\beta,\gamma)$.
- $F(\beta+\gamma) \supset F(\beta,\gamma)$: abbiamo già $F \subset F(\beta+\lambda\gamma)$, quindi resta da mostrare che

$$\gamma, \beta \in F(\beta+\lambda\gamma).$$

  - $\gamma \in F(\beta+\lambda\gamma)$:

    Abbiamo che $g(x) = 0$ per $x = \gamma$ (g è il polinomio minimo di γ e $g \in F[x] \subset F(\beta+\lambda\gamma)[x]$).

    Inoltre $f(\beta+\lambda\gamma-\lambda x) = 0$ per $x = \gamma$ (f è il polinomio minimo di β e $f \in F[x] \in F(\beta+\lambda\gamma)[x]$).

    Consideriamo dunque $h(x) := MCD(g(x), f(\beta+\lambda\gamma-\lambda x)) \in F(\beta+\lambda\gamma)[x]$.
    Osserviamo che $h(x) \neq 1$, infatti se lo fosse esisterebbero due polinomi $A(x), B(x) \in F(\beta+\lambda\gamma)[x]$ tali che

$$A(x)g(x) + B(x)f(\beta+\lambda\gamma-\lambda x) = 1,$$

    ma per $x = \gamma$ dovrebbe valere 0+0=1. Analogamente si verifica che $h(x) \neq c$ con c costante.

    Osserviamo anche che $\deg(h) \neq d$ con $d > 1$, si mostra supponendo per assurdo che $deg(h) > 1$. Poichè vale $h(x)|g(x)$ allora esiste $j \in \{2,\dots,m\}$ tale che γ_j è radice di h. Vale inoltre che $h(x)|f(\beta+\lambda\gamma-\lambda x)$, dunque γ_j è anche radice di $f(\beta+\lambda\gamma-\lambda x)$.

    Abbiamo dunque $f(\beta+\lambda\gamma-\lambda\gamma_j) = 0$, ma, essendo β_i le radici di f, ciò si verifica se e solo se esiste $i \in \{1,...,l\}$ tale che $\beta_i = \beta+\lambda\gamma-\lambda\gamma_j$, che è assurdo per (2.3).

    Quindi abbiamo mostrato che $\deg(h) = 1$ e, essendo γ radice di g e di $f(\beta+\lambda\gamma-\lambda x)$

$$\Rightarrow h(x) = x-\gamma \in F(\beta+\lambda\gamma)[x]$$

$$\Rightarrow \gamma \in F(\beta+\lambda\gamma).$$

  - $\beta \in F(\beta+\lambda\gamma)$:

$$\gamma, \beta + \lambda\gamma \in F(\beta + \lambda\gamma),\ \lambda \in F \Rightarrow \beta = \beta + \lambda\gamma - \lambda\gamma \in F(\beta + \lambda\gamma).$$

Abbiamo dunque concluso la dimostrazione di (2.4), quindi resta da mostrare che

$$\beta + \lambda\gamma \text{ è separabile su } F. \tag{2.5}$$

Cioè che, dato $p(x) \in F[x]$ il suo polinomio minimo, p è separabile.

A questo fine introduciamo ora un polinomio $s(x)$, verificheremo su questo che:

(i) $\beta + \lambda\gamma$ sia radice di s,

(ii) $s(x) \in F[x]$,

(iii) $p|s$ in $F[x]$ e che

(iv) s abbia tutte radici distinte.

Tutto ciò ci permetterà di dimostrare che il polinomio p è separabile, e dunque che anche $\beta + \lambda\gamma$ lo è a sua volta.

Innanzitutto definiamo $s(x)$ come

$$s(x) := \prod_{j=1}^{m} f(x - \lambda\gamma_j).$$

(i) Diciamo che s ha radice $\beta + \lambda\gamma$, infatti

$$\begin{aligned} s(\beta + \lambda\gamma) &= \prod_{j=1}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) = \\ &= f(\beta + \lambda\gamma - \lambda\gamma) \prod_{j=2}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) = \\ &= f(\beta) \prod_{j=2}^{m} f(\beta + \lambda\gamma - \lambda\gamma_j) = 0. \end{aligned}$$

(ii) Per dimostrare che $s(x) \in F[x]$ faremo uso della teoria dei polinomi simmetrici, come visto nel Capitolo 1.4, inizialmente definiamo un

polinomio ausiliare

$$\xi(x) := \prod_{j=1}^{m} f(x - x_j).$$

Osserviamo che permutando le x_j questo rimane invariato, cioè è simmetrico.

Per il teorema di Newton (Teorema 1.3.1) vale dunque che i coefficienti di ξ(x) sono polinomi simmetrici in $x_1, ..., x_n$, cioè

$$\xi(x) = \sum_{i=0}^{lm} \sigma_i(x_1, ..., x_m)x^i.$$

Ragionando ora in modo analogo su $s(x)$ possiamo scrivere

$$s(x) = \sum_{i=0}^{lm} \sigma_i(\lambda\gamma_1, ..., \lambda\gamma_m)x^i.$$

Dunque, grazie al Corollario 1.3.2, possiamo dire che $s(x)$ assume valori in F.

(iii) Osserviamo che $\beta+\lambda\gamma$ è radice di p e di s, inoltre p è il suo polinomio minimo, allora $p|s$ in $F[x]$.

(iv) Vediamo che s ha radici distinte. Fattorizzando f nel suo campo di spezzamento otteniamo

$$f(x) = (x - \beta)(x - \beta_2) \cdots (x - \beta_l) = \prod_{i=1}^{l}(x - \beta_i). \tag{2.6}$$

Sostituiamo ora (2.6) nella definizione di s

$$s(x) = \prod_{j=1}^{m}\prod_{i=1}^{l}(x - \lambda\gamma_j - \beta_i) = \prod_{j=1}^{m}\prod_{i=1}^{l}(x - (\lambda\gamma_j + \beta_i)).$$

Grazie a (2.1) deduciamo che tutte le radici di s sono distinte e poichè $p|s$ allora anche s ha tutte radici distinte.

Segue che p è separabile e dunque anche $\beta + \lambda\gamma$ è separabile, cioè ho concluso la verifica di (2.5).

Avendo verificato (2.4), (2.5) e posti $t_1 := 1$ e $t_2 := \lambda$ abbiamo dimostrato il teorema per $n = 2$.

n-1⇒ n Supponiamo che il teorema valga per $n-1$, mostreremo che da ciò segue il teorema per n.

Dato $L = F(\alpha_1, ..., \alpha_{n-1})$, con α_i separabili per ogni $i = 1, ..., n-1$, esistono $t_1, ..., t_{n-1} \in F$ tali che $\alpha_0 := t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}$ sia separabile e che $L = F(\alpha_1, ..., \alpha_{n-1}) = F(\alpha_0)$.

Consideriamo dunque $L' := F(\alpha_1, ..., \alpha_n)$:

$$\begin{aligned} L' = F(\alpha_1, ..., \alpha_n) = F(\alpha_1, ..., \alpha_{n-1})(\alpha_n) = \\ = L(\alpha_n) = F(\alpha_0)(\alpha_n) = F(\alpha_0, \alpha_n). \end{aligned}$$

Cioè ci riportiamo al caso $n = 2$, che abbiamo già dimostrato, dunque esiste $\alpha = \alpha_0 + t\alpha_n$, con $t \in F$, tale che α è separabile e $F(\alpha_0, \alpha_n) = F(\alpha)$.

Così abbiamo concluso la dimostrazione sotto ipotesi che F sia un campo infinito, procederemo nella prossima sezione a dimostrare il teorema nel caso di F campo finito.

2.3 Dimostrazione su F campo finito

Per procedere con la dimostrazione, sotto ipotesi di campo finito, è necessario introdurre un Lemma, che dimostriamo. Per precisazioni e approfondimenti riguardo a questo lemma ci si riferisce a [2].

Lemma 2.3.1. *Ogni A sottogruppo finito di un gruppo moltiplicativo di un campo è ciclico.*

Dimostrazione. Ricordiamo che se $a, b \in A$ sono elementi di periodo rispettivamente α, β, allora esiste $c \in A$ di periodo $\gamma = mcm(\alpha, \beta)$.

Siano $m := |A|$ e m':= "massimo ordine degli elementi di A".
Possiamo mostrare che $\forall$ a$\in$ A $a^{m'}$=1. Se supponiamo che esista $b \in A$ di ordine β tale che $b^{m'} \neq 1$, allora segue che $\beta \nmid m'$, ma questo implicherebbe che $mcm(\beta, m') > m'$ e ciò è assurdo per la massimalità di m'.

Consideriamo ora l'equazione $x^{m'} - 1 = 0$, questa ha al più m' soluzioni, e tutti gli elementi di A sono tra queste, allora $m \leq m'$. Ora m' è l'ordine di un elemento di A, dunque $m'|m = |A|$ e quindi $m = m'$.

Perciò abbiamo dimostrato che A è ciclico in quanto abbiamo trovato un suo elemento di ordine pari a quello di A. □

Torniamo dunque alla dimostrazione. Sia F un campo finito, $L|F$ è una estensione di campi finita, quindi L è campo finito e inoltre L^* è un gruppo ciclico per il Lemmma 2.3.1.

Sia α un generatore di L^*, vedremo che questo è proprio l'elemento primitivo del teorema.

Mostriamo inizialmente che

$$\alpha \text{ è separabile.} \tag{2.7}$$

Sia $m := |L| - 1$, e quindi $\alpha^m = 1$. Per ogni $i \in \{0, ...m-1\}$ α^i è radice di $f(x) = x^m - 1$, scriviamo

$$f(x) = (x-1)(x-\alpha)\cdots(x-\alpha^{m-1}).$$

Il campo L è proprio il campo di spezzamento di f ed f è separabile, infatti gli α^i sono distinti per $i \in \{0, ..., m-1\}$. Se f è separabile lo sono anche le sue radici e in particolare α è separabile.

Resta da mostrare che

$$L = F(\alpha). \tag{2.8}$$

Verifico le due inclusioni di (2.8).

$\subseteq$: $F(\alpha)$ contiene tutte le potenze di α, quindi contiene tutti gli elementi di L^*, contiene anche lo zero in quanto è un campo.

$\supseteq$: $\alpha \in L$ e $F \subset L$ dunque $L \supseteq F(\alpha)$ che è il più piccolo campo che contiene F e α.

Con ciò si completa la dimostrazione del teorema dell'elemento primitivo.

CAPITOLO 3

Applicazione in Teoria dei Numeri

In questo capitolo vogliamo contestualizzare il teorema dell'elemento primitivo nell'ambito della teoria dei numeri, in particolare come strumento utile allo studio dei campi di numeri (*number fields*), cioè le estensioni finite di $\mathbb{Q}$.

A questo fine presenteremo alcuni concetti, quali appunto i campi di numeri e le immersioni di un campo di numeri in $\mathbb{Q}$, cioè i morfismi di campo che portano gli elementi di un campo di numeri nella chiusura algebrica di $\mathbb{Q}$.

Inoltre enunceremo di nuovo il teorema dell'elemento primitivo con delle ipotesi diverse, più precisamente questo enunciato richiederà di avere un'estensione finita di un campo di caratteristica 0. Vedremo poi come queste sono ipotesi sufficienti a riportarci al teorema classico.

In seguito accenneremo ad alcune conseguenze del teorema sui campi di numeri.

Per la stesura di questo capitolo si fa riferimento principalmente a [6] per le definizione e l'enunciato del teorema e a [8] per qualche chiarimento. La dimostrazione di questo è stata prodotta usando i concetti e teoremi esposti nel Capitolo 1 e le nozioni studiate nella stesura di questo elaborato.

3.1 Campi di Numeri

Definizione 3.1. (Campo di Numeri) Un campo di numeri, o number field è un'estensione finita di $\mathbb{Q}$.

Il grado di un campo di numeri K è definito come $\deg(K) := [K : \mathbb{Q}]$.

Osservazione 2. Grazie alla Proposizione 1.1.1 possiamo osservare che ogni campo di numeri è un'estensione algebrica di $\mathbb{Q}$.

Esempio 3.1.1. (i) Un esempio banale di campo di numeri è proprio $\mathbb{Q}$, questo è evidentemente un'estensione di sè stesso e dunque un campo di numeri con grado 1.

(ii) Consideriamo l'estensione finita $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ di $\mathbb{Q}$, come nell'Esempio 1.1.1. Questo è un campo di numeri, inoltre si può dimostrare che $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. (Si trova tale dimostrazione in [3, Example 4.3.9, p. 92])

(iii) Un controesempio è il campo $\mathbb{R}$ estensione di $\mathbb{Q}$, infatti questa ha grado infinito, $[\mathbb{R} : \mathbb{Q}] = \infty$, dunque non può essere un campo di numeri.

3.2 Immersioni

Il concetto di $\mathbb{Q}$ immersione di un campo di numeri ci servirà per osservare alcune conseguenze al teorema dell'elemento primitivo.

Definizione 3.2. ($\mathbb{Q}$ Immersione di un Campo di Numeri) Sia K un campo di numeri, una $\mathbb{Q}$ immersione di K è un morfismo di campi

$$\sigma : K \longrightarrow \overline{\mathbb{Q}}$$

tale che $\sigma_{|\mathbb{Q}} = Id$.

Denotiamo con $Mor_{\mathbb{Q}}(K)$ l'insieme delle $\mathbb{Q}$ immersioni di K.

Esempio 3.2.1. Ovviamente dato un qualsiasi campo di numeri K l'applicazione identità, $Id : K \longrightarrow K$, è una $\mathbb{Q}$ immersione di K.

3.3 Teorema

Riprendiamo ora il teorema dell'elemento primitivo. In seguito evidenzieremo le conseguenze immediate che ha questo enunciato sui campi di numeri.

Teorema 3.3.1. *Sia $L|K$ estensione finita con* $\mathrm{ch}(K) = 0$ *allora esiste un elemento $\alpha \in L$ tale che $L = K(\alpha)$.*

Dimostrazione. Per dimostrarlo vedo che queste ipotesi sono equivalenti a quelle del teorema classico nel caso di un campo infinito. Servono quindi:

(i) K infinito.

(ii) $L = K(\alpha_1, ..., \alpha_n)$ con α_i separabili.

(i) Poichè $\mathrm{ch}(K) = 0$ dunque K contiene un sottocampo isomorfo a $\mathbb{Q}$. Infatti dato M un campo qualsiasi e C il suo sottocampo minimale contenente l'unità 1, il campo C dipende dalla caratteristica di M, in particolare poichè $\mathrm{ch}(M) = 0$ allora C è isomorfo a $\mathbb{Q}$, mentre se $\mathrm{ch}(M) = p$ primo allora C è isomorfo ad un campo finito. (cf. [5])

(ii) Poichè $L|K$ è un'estensione finita, allora esistono α_i finiti tali che $L = K(\alpha_1, ..., \alpha_n)$.

Quindi, grazie alla Proposizione 1.1.1, L è anche un'estensione algebrica di K e in particolare anche gli α_i sono algebrici. Dunque, per la Proposizione 1.2.1, possiamo affermare che i polinomi minimi degli α_i sono irriducibili. Dal Teorema 1.4.3 segue che questi sono anche separabili e dunque lo sono anche gli α_i. □

Osservazione 3. Ora, sapendo che $\mathrm{ch}(\mathbb{Q}) = 0$, possiamo subito affermare che ogni campo di numeri ha un elemento primitivo, cioè ogni campo di numeri è un'estensione semplice.

3.4 Conseguenze

Sia K un campo di numeri, per il teorema dell'elemento primitivo, come osservato, esiste un elemento primitivo $\alpha \in K$ tale che

$$K = \mathbb{Q}(\alpha).$$

Sia ora $M(x) \in \mathbb{Q}[x]$ il polinomio minimo di α su $\mathbb{Q}$. Sia il suo grado $n := \deg(M)$, osserviamo che

$$[K : \mathbb{Q}] = n.$$

Osserviamo ora che $M(x)$ è irriducibile, grazie alla Proposizione 1.2.1, in quanto è il polinomio minimo di α che è algebrico su $\mathbb{Q}$ (Osservazione 2), quindi per il Teorema 1.2.3 è separabile, cioè ha tutte radici distinte.

Ora, poichè $K = \mathbb{Q}(\alpha)$, allora ogni $\mathbb{Q}$ immersione σ di K in $\mathbb{Q}$ è completamente determinata da $\sigma(\alpha)$.

Osserviamo che $M(\alpha) = 0$ e $\sigma_{|\mathbb{Q}} = id$, questo per la definizione di $\mathbb{Q}$ immersione e per la scelta di M, allora anche $\sigma(\alpha)$ è una radice di M (avremo $\sigma(\alpha) \neq \alpha$ quando $\sigma \neq id$). In particolare si può vedere come $Mor_{\mathbb{Q}}$ è in biiezione con le radici di M.

Cioè, considerate le n radici distinte di M, $\alpha_1 = \alpha, \ldots, \alpha_n$, possiamo associare ad ognuna delle α_i la $\mathbb{Q}$ immersione σ tale che

$$\begin{aligned} \sigma \colon K &\to \overline{\mathbb{Q}} \\ \alpha &\mapsto \sigma_i(\alpha) = \alpha_i. \end{aligned}$$

Dunque questo campo di numeri K può essere immerso in $\overline{Q}$ in n modi diversi.

Bibliografia

[1] Caranti A., *Note per un corso di Algebra per 12 crediti complessivi*, reperibili in pdf presso `http://www.science.unitn.it/~caranti/Didattica/Algebra/static/Note/Algebra.pdf`.

[2] Cicalò S., de Graaf W.A., *Teoria di Galois*, Aracne Editrice, 2008, Italia.

[3] Cox D.A., *Galois Theory*, John Wiley & Sons, 2012, Hoboken, NJ .

[4] D'Andrea A. , *Algebra 2 – Lezioni dal 16 Dicembre 2003 AL 21 Gennaio 2004*, reperibili in pdf presso `http://www1.mat.uniroma1.it/people/dandrea/didattica/algebra2-04/alg03_4.pdf`.

[5] Del Corso I., *Caratteristica di un campo*, 2016/2017, reperibile in pdf presso `http://www.dm.unipi.it/~delcorso/Ilaria%20DEL%20CORSO_files/aritmetica/campi_finiti.pdf`.

[6] Ellia P., *Teoria dei Numeri*, 2013-2014, reperibile in pdf presso `http://dm.unife.it/philippe.ellia/Docs/TeoriaNumeri2013-14-OnLine.pdf`.

[7] Gabelli S., *Teoria delle Equazioni e Teoria di Galois*, Springer-Verlag, 2008, Milano, Italia.

[8] Stein W., *Algebraic Number Theory, a Computational Approach*, November 14, 2012, reperibile in pdf presso `http://wstein.org/books/ant/ant.pdf`.