Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Matematica

Il Teorema dell'Elemento Primitivo e le sue Applicazioni

Tesi di Laurea in
Complementi di Algebra 1

Relatore:
Chiar.mo Prof.
Luca Migliorini

Presentata da:
Lucia Traini

Sessione seconda
Anno Accademico
2010/2011

La preoccupazione dell'uomo e del suo destino deve sempre costituire l'interesse principale di tutti gli sforzi tecnici. Non dimenticatelo mai, in mezzo ai vostri diagrammi ed alle vostre equazioni.

Albert Einstein

Indice

Introduzione

Il Teorema dell'Elemento Primitivo è un risultato di teoria dei campi, che afferma che, sotto opportune ipotesi, un'estensione di campi ottenuta aggiungendo n elementi al campo di partenza è uguale all'estensione ottenuta aggiungendo al medesimo campo un solo elemento (detto appunto primitivo) opportunamente scelto. Questo dà notevoli vantaggi in quanto riduce la considerazione di estensioni finite a estensioni semplici, ottenute cioè aggiungendo un elemento. In realtà il teorema è implicitamente usato anche nell'algebra più elementare, nella manipolazione di espressioni contenenti radici di polinomi a coefficienti razionali, come vedremo nell'ultimo capitolo.

In questa tesi verrà presentato e dimostrato accuratamente il teorema, inoltre sarà fornito un esempio di una semplice applicazione.

Questo elaborato si compone di tre capitoli:

- ▷ **Nozioni Preliminari**: si compone di tre sezioni; nella prima vengono date le definizioni delle strutture algebriche di base, necessarie per poter comprendere l'enunciato e la dimostrazione del teorema centrale, con particolare attenzione alle estensioni di campi. Il secondo paragrafo tratta dei polinomi; il terzo infine enuncia alcuni risultati dell'algebra la cui padronanza è fondamentale nello studio dell'argomento di questa tesi.

- ▷ **Il Teorema dell'Elemento Primitivo**: contiene l'enunciato del teorema e la sua dimostrazione, suddivisa in due sezioni, nella prima si tratta il caso di un campo di caratteristica 0, ossia di infiniti elementi, la seconda invece riguarda i campi finiti.

- ▷ **Esempi e Applicazioni**: Si considera un esempio noto, ovvero l'estensione di $\mathbb{Q}$ con una radice sesta dell'unità e si mostra che ciò è in pieno accordo con il teorema dell'elemento primitivo. In seguito si passa alle applicazioni: quella trattata è la

Capitolo 1

Nozioni Preliminari

Questo primo capitolo ha lo scopo di introdurre alcuni concetti e risultati dell'algebra che sono fondamentali per la comprensione della tesi e dell'importanza del teorema che tratteremo.

1.1 Strutture Algebriche

Definizione 1.1. Un **monoide** è un insieme M dotato di un'operazione binaria detta prodotto che associa alla coppia (a, b) di elementi di M l'elemento $a * b$, e tale che ha le seguenti proprietà:

- M è chiuso rispetto al prodotto, ossia $\forall\ (a, b) \in M \times M$ il prodotto $a * b \in M$
- il prodotto è associativo in M, ossia $a * (b * c) = (a * b) * c\ \forall a, b, c \in M$
- M possiede un elemento neutro per il prodotto, ossia $\forall a \in M\ \exists\ 1_M \in M$ t.c. $a * 1_M = a$.

A partire dalla struttura di monoide, che indicheremo con $(M, *, 1_M)$, definiamo ora le strutture di gruppo, anello e campo.

Definizione 1.2. Un **gruppo** è una struttura $(G, *, 1_G, ')$, o più semplicemente $(G, *)$, che si differenzia dal monoide per il fatto che l'insieme G contiene anche il simmetrico (o inverso) x' di ogni elemento x, cioè $\forall\ x \in G\ \exists\ x' \in G$ t.c. $x * x' = 1$.
Un gruppo è detto **abeliano** se l'operazione gode della proprietà commutativa.

Consideriamo ora un gruppo moltiplicativo G. È detto **gruppo ciclico** se tutti i suoi elementi si possono scrivere come potenze di un generatore, ossia se $\exists\ \xi \in G$ t.c. $G = \{\xi^k | k \geq 0\}$. Se $\exists\ n > 0$ t.c $\xi^n = 1$ e n è il più piccolo per cui si verifica questo, allora n è detto l'**ordine** di G e G è quindi un gruppo finito.
Analogamente, si dice ordine di un elemento $\vartheta \in G$ il più piccolo intero $m > 0$ t.c. $\vartheta^m = 1$; nel caso di gruppi finiti abbiamo che l'ordine di un qualsiasi elemento del gruppo divide l'ordine del gruppo, e come conseguenza del teorema di Lagrange questo vale anche per l'ordine di un qualsiasi sottogruppo (cfr: Artin, Algebra, cap. 2).

Definizione 1.3. Un **anello** è una struttura $(A, +, *, 1_A)$ dove $(A, +)$ è un gruppo abeliano, $(A, *, 1_A)$ è un monoide e valgono le seguenti proprietà distributive dell'operazione $+$ rispetto a $*$:

- $(a + b) * c = a * c + b * c\ \forall\ a, b, c \in A$
- $a * (b + c) = a * b + a * c\ \forall\ a, b, c \in A$

L'anello si dice **commutativo** se l'operazione $*$ è commutativa.

Definizione 1.4. Un **campo** è un anello commutativo in cui ogni elemento non nullo ha un simmetrico.

Possiamo a questo punto definire uno spazio vettoriale:

Definizione 1.5. Sia K un campo il cui prodotto interno è indicato con $\cdot$. Sia V un insieme non vuoto chiuso rispetto ad un'operazione binaria $+$ per la quale $(V, +)$ è un gruppo abeliano e sia definita una funzione $* : K \times V \to V$ detta *moltiplicazione per scalare* che abbia le seguenti proprietà:

- associatività: $\forall\ a, b \in K,\ \forall\ v \in V\ a * (b * v) = (a \cdot b) * v$
- elemento neutro: $\forall\ v \in V\ 1 * v = v$ (dove 1 è l'elemento neutro di K)

- distributività rispetto ai vettori: $\forall\ a \in K,\ \forall\ u, v \in V\ a * (u + v) = a * u + a * v$
- distributività rispetto agli scalari: $\forall\ a, b \in K,\ \forall\ v \in V\ (a + b) * v = a * v + b * v$

Allora diciamo che V è un **K-spazio vettoriale**, gli elementi di V si chiamano vettori e gli elementi di K scalari.
Una n-upla di vettori $\{v_1, \ldots, v_n\}$ si dice linearmente indipendente se $\exists\ k_1, \ldots, k_n \in K$ t.c. $k_1v_1 + \ldots + k_nv_n = 0 \iff k_i = 0\ \forall\ i = 1, \ldots, n$.
L'insieme $\{v_1, \ldots, v_n\}$ di vettori di V è un **insieme di generatori** del K-spazio vettoriale V se ogni vettore $v \in V$ può essere scritto come loro combinazione lineare. Una **base** di uno spazio vettoriale è per definizione un insieme di vettori linearmente indipendenti che generano lo spazio.

Abbiamo introdotto queste nozioni fondamentali dell'algebra per poter definire la struttura principale per il lavoro di questa tesi: l'estensione di campi.

Definizione 1.6. Un dato campo K può avere uno o più **sottocampi**: sottoinsiemi di K che a loro volta, con le operazioni indotte, possiedono le proprietà di campo. In questo caso, se F è uno di tali sottoinsiemi, diciamo anche che $F \subset K$ è un'**estensione di campi** (abbreviamo in e.c.).
Data una estensione $F \subset K$, e n elementi $\alpha_1, \ldots, \alpha_n \in K$ non appartenenti a F, possiamo costruire un'estensione $F \subset F(\alpha_1, \ldots, \alpha_n) \subset K$ che è il più piccolo campo che contiene F e gli elementi $\alpha_1, \ldots, \alpha_n$.
Risulta evidente che un'e.c. $F \subset K$ ha una struttura di F-spazio vettoriale, e diciamo che $F \subset K$ e.c. **finita** se $dim_F K < \infty$; in questo caso il grado dell'estensione è $dim_F K := [K : F]$.

Definizione 1.7. Sia $F \subset K$ e.c. Un elemento $\alpha \in K$ è **algebrico** su F se nell'anello $F[x]$ esiste un polinomio che si annulli in α.

1.2 Polinomi

La definizione appena conclusa ci permette di darne un'altra, quella di **campo di spezzamento** di un polinomio, che è l'esempio di estensione di campi che più useremo in questo elaborato.

Definizione 1.8. Dato un polinomio $f(x) \in F[x]$, il suo campo di spezzamento è un campo L contenente F come sottocampo, tale che:

- $f(x)$ spezza interamente in fattori di primo grado se considerato come polinomio a coefficienti in L;
- $L = F(\gamma_1, \ldots, \gamma_n)$ dove $\gamma_1, \ldots, \gamma_n$ sono le radici di $f(x)$;
- L è il più piccolo campo in cui ciò avviene.

Definizione 1.9. Sia F un campo, K una sua estensione, sia $\alpha \in K$; il **polinomio minimo** di α su F è il polinomio $p_\alpha \in F[x]$ monico e irriducibile che si annulla in α (e che pertanto divide ogni altro polinomio $g \in F[x]$ t.c. $g(\alpha) = 0$).
È evidente che tale polinomio esiste se e solo se α è algebrico in F

Definizione 1.10. Sia F un campo; un elemento $\alpha \in F$ è **separabile** se lo è il suo polinomio minimo, cioè se quest'ultimo non ha radici multiple nel suo campo di spezzamento.

1.3 Risultati Notevoli

In questa sezione presenteremo due risultati dell'algebra che useremo nel prossimo capitolo per la dimostrazione del Teorema dell'Elemento Primitivo.

1.3.1 Identità di Bezout

Definizione 1.11. Dati due polinomi f, g a coefficienti in un campo F, un MCD dei due è un polinomio $h := MCD(f, g)$ t.c.:

i. $h \mid f$ e $h \mid g$

ii. se esiste un altro polinomio h' con la proprietà *i* allora $h' \mid h$

Lemma 1.3.1 (Identità di Bezout)**.** *Siano f, g polinomi non nulli a coefficienti in F, e sia $h = MCD(f, g)$. Allora esistono due polinomi t, z tali che: $ft + gz = h$.*

La dimostrazione di questo è diretta conseguenza dell'algoritmo euclideo delle divisioni successive, che vale nell'anello dei polinomi a coefficienti in un campo qualunque.

1.3.2 Funzioni Simmetriche Elementari

Definizione 1.12. Siano $x_1, \ldots, x_n$variabili di polinomi a coefficienti in un campo F. Definiamo le **funzioni simmetriche elementari**:

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{n} x_i \\
\sigma_2 &= \sum_{i<j} x_i x_j \\
&\vdots \\
\sigma_r &= \sum_{i_1<\ldots<i_r} x_{i_1} \ldots x_{i_r} \\
&\vdots \\
\sigma_n &= \prod_{i=1}^{n} x_i
\end{aligned}$$

Teorema 1.3.2 (Teorema di Newton)**.** *Ogni polinomio simmetrico in $F[x_1, \ldots, x_n]$ può essere scritto in modo unico come un polinomio nelle $\sigma_1, \ldots, \sigma_n$ a coefficienti in F.*

Dall'espressione dei coefficienti di un polinomio come funzioni elementari delle sue radici, segue immediatamente:

Corollario 1.3.3. *Sia $F \subset L$ una e.c., siano $\gamma_1, \ldots, \gamma_n \in L$ le radici di un polinomio a coefficienti in con F. Allora ogni polinomio simmetrico a coefficienti in F, calcolato su $\gamma_1, \ldots, \gamma_n$ assume valori in F.*

Capitolo 2

Il Teorema dell'Elemento Primitivo

Sia $L = F(\alpha_1, \ldots, \alpha_n)$ e.c. finita, dove $\alpha_1, \ldots, \alpha_n \in L$ sono separabili su F.
Allora $\exists\ \alpha \in L$ separabile su F t.c. $L = F(\alpha)$.
Inoltre, se F è infinito α puó essere scelto nella forma $\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n$ dove $t_1, \ldots, t_n \in F$.

2.1 Dimostrazione per campo infinito

Sia F un campo infinito,dimostriamo per induzione su n che $\exists\ t_1, \ldots, t_n \in F$ t.c. $\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n$ è separabile su F e $L = F(\alpha)$. Consideriamo il caso n=2, ossia $L = F(\beta, \gamma)$.
Consideriamo i polinomi minimi in F di β e γ:
sia $f \in F[x]$ il polinomio minimo di β, di grado l;
sia $g \in F[x]$ il polinomio minimo di γ, di grado m.
Poichè β, γ sono separabili, f ha l radici distinte $\beta_1 = \beta, \ldots, \beta_l$ e g ha m radici distinte $\gamma_1 = \gamma, \ldots, \gamma_m$.
Poichè F è infinito $\exists\ \lambda \in F$ t.c. $\lambda \neq \dfrac{\beta_i - \beta_r}{\gamma_s - \gamma_j}\ \forall\ i, r, s, j$ t.c. $1 \leq r, i \leq l,\ r \neq i, 1 \leq s,\ j \leq m,\ s \neq j$.

Questo fatto implica:

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

e quindi $\forall (r,s) \neq (i,j)$

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

In particolare, poichè avevamo posto $\beta = \beta_1$ e $\gamma = \gamma_1, \forall\ i \in \{2,\dots,l\},\ \forall\ j \in \{2,\dots,m\}$ vale

$$\beta_i \neq \beta + \lambda\gamma - \lambda\gamma_j \tag{2.2}$$

Andiamo ora a dimostrare che $F(\beta + \lambda\gamma) = F(\beta,\gamma)$.
È immediato verificare che $F(\beta + \lambda\gamma) \subseteq F(\beta,\gamma)$; infatti l'elemento $\beta + \lambda\gamma \in F(\beta,\gamma)$ perchè quest'ultimo è un campo cui β,γ appartengono, e $\lambda \in F$, pertanto l'estensione $F(\beta + \lambda\gamma)$ deve necessariamente essere contenuta in $F(\beta,\gamma)$.
Per provare l'inclusione inversa dobbiamo vedere che $\beta,\gamma \in F(\beta + \lambda\gamma)$.
Iniziamo considerando γ.
Abbiamo che:

- $g(x) = 0$ per $x = \gamma$, perchè g è polinomio minimo di γ, e $g \in F[x] \subset F(\beta + \lambda\gamma)[x]$.
- $f(\beta + \lambda\gamma - \lambda x) = 0$ per $x = \gamma$ perchè f è polinomio minimo di β, e $f(\beta + \lambda\gamma - \lambda x) \in F[x] \subset F(\beta + \lambda\gamma)[x]$.

Consideriamo il $MCD(g(x), f(\beta + \lambda\gamma - \lambda x))$:
se $MCD(g(x), f(\beta + \lambda\gamma - \lambda x)) = 1$ allora per l'identità di Bezout nell'anello $F(\beta + \lambda\gamma)[x]$ esisterebbero due elementi $A(x), B(x)$ tali che $A(x)g(x) + B(x)f(\beta + \lambda\gamma - \lambda x) = 1$, ma per $x = \gamma$ si avrebbe $A(x)0 + B(x)0 = 1 \iff 0 = 1$, e questo è un assurdo.
Per lo stesso motivo il $MCD(g(x), f(\beta + \lambda\gamma - \lambda x))$ non puó essere una costante, pertanto sarà un polinomio $h(x) \in F(\beta + \lambda\gamma)[x]$ di grado positivo.
Dimostriamo che $deg(h(x)) = 1$.
Se per assurdo fosse $deg(h(x)) > 1$, a motivo della separabilità di g, nel campo di spezzamento di quest'ultimo avremmo:
$g(x) = (x - \gamma)(x - \gamma_2)\cdots(x - \gamma_m)$, e si evince che dovrebbe esistere $r \leqslant m$ t.c.

$$h(x) = \prod_{k=1}^{r}(x - \gamma_k)$$

.
Questo implicherebbe l'esistenza di $j \in \{2, \dots, m\}$ t.c. γ_j sia radice di h, e di conseguenza, siccome h divide $f(\beta + \lambda\gamma - \lambda x)$, γ_j sarebbe radice anche di quest'ultimo, cioè $f(\beta + \lambda\gamma - \lambda\gamma_j) = 0$ e quindi $\beta + \lambda\gamma - \lambda\gamma_j$ risulterebbe essere una delle radici di f, sia β_i, e si avrebbe $\beta_i = \beta + \lambda\gamma - \lambda\gamma_j$, ma questo è un assurdo perchè contraddice 2.2.
Pertanto h non puó che essere di primo grado, e in particolare $h = x - \lambda\gamma$ per la separabilità di g e perchè h divide g e $f(\beta + \lambda\gamma - \lambda x)$.
Poichè h è di primo grado e γ ne è una radice, abbiamo provato che $\gamma \in F(\beta + \lambda\gamma)$.
A questo punto $\beta = (\beta + \lambda\gamma) - \lambda\gamma \in F(\beta + \lambda\gamma)$ in quanto combinazione lineare di suoi elementi.
Abbiamo pertanto provato che $F(\beta, \gamma) \subseteq F(\beta + \lambda\gamma)$, e questo conclude la dimostrazione che $F(\beta + \lambda\gamma) = F(\beta, \gamma)$. Vediamo ora che il polinomio minimo di $\beta + \lambda\gamma$ su F[x], sia p, è separabile: consideriamo

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

una cui radice è $\beta + \lambda\gamma$, infatti:

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

poichè β è radice di f.
Vediamo ora che $s(x) \in F[x]$.
Consideriamo il seguente polinomio:

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

Osserviamo che $S(x) \in F[x_1, \dots, x_m][x]$ e che permutando le x_j il polinomio rimane invariato; questo significa che i coefficienti di S sono polinomi simmetrici nelle variabili

$x_1, \ldots, x_n$, cioè possiamo scrivere

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

dove le σ_i sono funzioni simmetriche elementari nelle incognite $x_1, \ldots, x_m$, come definito in 1.12.
Allora, tornando al polinomio di partenza, $s(x)$, abbiamo che:

$$s(x) = \sum_{i=0}^{lm} \sigma_i(\lambda_\gamma 1, \ldots, \lambda_\gamma m)x^i$$

e quindi per il corollario 1.3.3 possiamo concludere che $s(x) \in F[x]$.
Poichè $s(x)$ si annulla in $\beta + \lambda\gamma$ e p è il polinomio minimo di $\beta + \lambda\gamma$, nell'anello $F[x]$ avviene che p divide $s(x)$.
Spostiamoci ora nel campo di spezzamento di f: qui il polinomio ha l radici distinte e, come detto precedentemente, spezza interamente in fattori di primo grado, pertanto:

$$\begin{aligned} s(x) &= \prod_{j=1}^{m} f(x - \lambda\gamma_j) \\ &= \prod_{j=1}^{m} \prod_{i=1}^{l} (x - \beta_i + \lambda\gamma_j) \end{aligned}$$

Per (2.1) s ha radici distinte, pertanto possiamo dire che p è separabile, in quanto divide s. Abbiamo quindi dimostrato che $\beta + \lambda\gamma$ è separabile in $F[x]$.
Ponendo $t_1 = 1$ e $t_2 = \lambda$ abbiamo provato il teorema per un campo F infinito e n=2.
Passiamo ora alla dimostrazione per il caso generale, sempre su un campo infinito.
Sia il teorema valido per $L = F(\alpha_1, \ldots, \alpha_{n-1})$ e consideriamo l'estensione $L' = F(\alpha_1, \ldots, \alpha_n)$, dove ogni elemeto α_i è separabile su F.
Per l'ipotesi induttiva esistono $n-1$ elementi di F, siano $t_1, \ldots, t_{n-1}$, tali che $\alpha_0 = t_1\alpha_1 + \ldots + t_{n-1}\alpha_{n-1}$ è separabile su F e $F(\alpha_1, \ldots, \alpha_{n-1}) = F(\alpha_0)$.
Ora, $F(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = F(\alpha_0, \alpha_n)$ e per quanto dimostrato precedentemente esiste un elemento $t \in F$ tale che $\alpha = \alpha_0 + t\alpha_n$ è separabile su F e $F(\alpha_0, \alpha_n) = F(\alpha)$.
Questo conclude la dimostrazione nel caso in cui F sia un campo infinito.

2.2 Dimostrazione per campo finito

Lemma 2.2.1. *Ogni A sottogruppo finito di un gruppo moltiplicativo di un campo è ciclico.*

Dimostrazione. Ricordiamo intanto che se $a,\ b$ sono due elementi di A di periodi rispettivamente α, β allora $\exists\ c \in A$ di periodo $\gamma = mcm(\alpha, \beta)$.
Ora, sia $m = |A|$ e sia m' il più alto ordine di un elemento di A, allora $\forall\ a \in\ A$ si ha $a^{m'} = 1$: infatti se ci fosse in A un elemento b di ordine β t.c. $b^{m'} \neq 1$, allora necessariamente β non divide m', e il $mcm(\beta, m')$ risulterebbe maggiore di m', ma l'esistenza di un elemento di tale ordine andrebbe a contraddire la massimalità di m'.
Consideriamo l'equazione $x^{m'} - 1 = 0$: ha al più m' soluzioni e tutti gli elementi di A la soddisfano, questo ci dice che $m \leq m'$.
D'altra parte m' è l'ordine di un elemento di A, e quindi m' deve dividere m; possiamo pertanto concludere che $m = m'$ e che A è ciclico, perchè abbiamo appena dimostrato che esiste un elemento di ordine pari all'ordine del gruppo. □

Sia F un campo finito e $F \subset L$ e.c. finita, è immediato verificare che L è a sua volta un campo finito.
Per il lemma 2.2.1 anche L^* è gruppo ciclico, poichè è gruppo moltiplicativo di un campo finito.
Andiamo ora a verificare che $L = F(\alpha)$ con α separabile su F.
Sia $m = |L| - 1$, è evidente, per quanto abbiamo detto sui gruppi ciclici e per il fatto che $\alpha^m = 1$, che $\forall\ i \in 0, \ldots, m-1$, α^i è radice di $x^m - 1$. Quindi in L sono presenti tutte le radici di $x^m - 1$ e possiamo scrivere:

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

È quindi evidente che L è il campo di spezzamento di $x^m - 1$ e per quanto scritto sopra possiamo concludere che quest'ultimo è separabile, pertanto lo sono tutte le sue radici e in particolare α.
Questo conclude la dimostrazione del teorema.

Capitolo 3

Esempi e Applicazioni

3.1 Un'applicazione

Una delle conseguenze del teorema visto nel precedente capitolo è la razionalizzazione dei polinomi, resa possibile da un isomorfismo che ci apprestiamo a studiare.

Proposizione 3.1.1. *Sia K un campo e sia $F = K(\gamma)$.*
L'estensione $F \subseteq K$ è finita $\Longleftrightarrow$ γ è algebrico su F.
In particolare, in questo caso $[K : F]$ è pari al grado del polinomio minimo di γ su K.

Dimostrazione. Se l'estensione è finita, sia di grado m, consideriamo $K(\gamma)$ come F-spazio vettoriale: qui non ci sono più di m vettori linearmente indipendenti, pertanto $1+a_1\gamma+a_2\gamma^2+\ldots+a_m\gamma^m = 0$ perchè combinazione lineare di $m+1$ elementi. Considero quindi il polinomio $f(x) = 1 + a_1x + a_2x^2 + \ldots + a_mx^m$, ha coefficienti in K e si annulla in γ. Abbiamo quindi provato che γ è algebrico.
Viceversa, sia γ algebrico su F: l'isomorfismo $\varphi : F[x]/(p_\gamma) \longrightarrow F[\gamma]$ che approfondiremo in 3.1 è anche isomorfismo di F-spazi vettoriali, in quanto
$\varphi(a[g]) = \varphi(a)\varphi([g]) = a\varphi([g]),\ \forall\ [g] \in F[x]/(p_\gamma)$ e $\forall\ a \in F$.
Sia $m = deg(p_\gamma)$, allora $dim_F F[x]/(p_\gamma) = m$ e, indicando con ξ la classe di x nel quoziente, $(1, \xi, \xi^2, \ldots, \xi^m)$ ne è una base; allora $(\varphi(1), \varphi(\xi), \varphi(\xi^2), \ldots, \varphi(\xi)^n)$ è una base di $F[\gamma]$.

Poichè si verifica che $F[\gamma] = F(\gamma)$ abbiamo trovato una base di quest'ultimo con un numero finito di elementi, pertanto l'estensione è finita. □

Definizione 3.1. Sia $\alpha \in K$ un elemento algebrico su F, e sia K un'estensione di campi di F. Consideriamo il morfismo di valutazione in α, che associa ad ogni polinomio in $F[x]$ la sua valutazione in α:

$$\begin{aligned} \varphi : F[x] &\longrightarrow K \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

Denotiamo l'immagine di φ con $F[\alpha]$, che è il più piccolo anello che contiene F e α.

Proposizione 3.1.2. *Sia α un elemento algebrico su F e sia $p_\alpha(x) \in F[x]$ il suo polinomio minimo. Allora esiste un isomorfismo $\varphi : F[x]/(p_\alpha) \longrightarrow F[\alpha]$ per cui $F[\alpha]$ è un campo, dunque $F[\alpha] = F(\alpha)$.*
Inoltre vale un risultato più generale: siano $\alpha_1, \ldots, \alpha_n$ elementi algebrici di un'e.c. $K \subset F$. Allora $F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n)$

Dimostrazione. Consideriamo il morfismo di valutazione in α:

$$\begin{aligned} \varphi : F[x] &\longrightarrow K = F(\alpha) \\ g(x) &\longmapsto g(\alpha) \end{aligned}$$

L'immagine è $F[\alpha]$ per definizione. L'algebricità di α in F implica che φ non è iniettivo e dunque il nucleo non è l'ideale banale ma l'ideale generato da p_α, questo possiamo dirlo perchè $F[x]$ è un PID e p_α appartiene al nucleo ed è irriducibile. Applichiamo quindi il teorema universale di omomorfismo per gli anelli:

$$\begin{array}{ccc} F[x] & \xrightarrow{\varphi} & F(\alpha) \\ {\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle i} \\ F[x]/(p_\alpha) & \xrightarrow{\cong} & F[\alpha] \end{array} \tag{3.1}$$

L'irriducibilità di p_α garantisce la massimalità dell'ideale (p_α) e dà al quoziente la struttura di campo, pertanto anche $F[\alpha]$ è un campo, e poichè $F(\alpha)$ è isomorfo al campo dei

quozienti di $F[\alpha]$, allora $F[\alpha] = F(\alpha)$.
La definizione induttiva di $F[\alpha_1, \ldots, \alpha_n]$ e $F(\alpha_1, \ldots, \alpha_n)$ e il teorema dell'elemento primitivo, per quanto visto nella proposizione 3.1.1, provano anche il risultato generale. □

Abbiamo quindi trovato un isomorfismo tra $F(\alpha)$ e $F[x]/(p_\alpha)$, questo vuol dire che ogni espressione razionale nelle $\alpha_1, \ldots, \alpha_n$ può essere scritta come polinomio in una combinazione lineare delle stesse $\alpha_1, \ldots, \alpha_n$.

3.1.1 Un Esempio

Consideriamo il campo $\mathbb{Q}$ e la sua estensione $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

- $\sqrt{2}$ è algebrico e separabile su $\mathbb{Q}$, infatti il suo polinomio minimo è $p_{\sqrt{2}}(x) = x^2 - 2$ che nel suo campo di spezzamento, $\mathbb{Q}(\sqrt{2})$, spezza in $(x + \sqrt{2})(x - \sqrt{2})$;
- lo stesso vale per $\sqrt{3}$, il cui polinomio minimo $p_{\sqrt{3}}(x) = x^2 - 3$ ha come campo di spezzamento $\mathbb{Q}(\sqrt{3})$ e qui spezza in $(x + \sqrt{3})(x - \sqrt{3})$

Pertanto possiamo applicare il teorema e dire che $\alpha = \sqrt{2} + \sqrt{3}$ è l'elemento primitivo: infatti il suo polinomio minimo $p_{\sqrt{2}+\sqrt{3}}(x) = x^4 - 10x^2 + 1$ in questo campo spezza nei fattori lineari $(x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x + (\sqrt{2} + \sqrt{3}))(x + (\sqrt{2} - \sqrt{3}))$.

Usiamo l'isomorfismo 3.1.2 per razionalizzare l'elemento $\dfrac{1}{\sqrt{2} + \sqrt{3}} = \dfrac{1}{\alpha} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$:

$$\varphi : \mathbb{Q}[x]/(p_{\sqrt{2}+\sqrt{3}}) \longrightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

Consideriamo $p_{\sqrt{2}+\sqrt{3}}(x)$ e il polinomio associato al denominatore dell'elemento su cui operiamo, sia $h(x) = x$ e applichiamo l'algoritmo di Euclide delle divisioni successive, grazie al quale possiamo anche trovare il $MCD(p_{\sqrt{2}+\sqrt{3}}, h)$, che coincide con l'ultimo resto non nullo:

$$\begin{aligned}
&x^4 - 10x^2 + 1 \div x = x^3 - 10x + 1 \\
&x \div 1 = x \\
&\implies x^4 - 10x^2 + 1 = x(x^3 - 10x) + 1 \\
&\implies x^4 - 10x^2 + 1 - x(x^3 - 10x) = 1
\end{aligned}$$

Per l'identità di Bezout (1.3.1) quest'ultima equazione vale anche per la valutazione in $\alpha = \sqrt{2} + \sqrt{3}$:

$$\begin{aligned} &\alpha^4 - 10\alpha^2 + 1 - \alpha(\alpha^3 - 10\alpha) = 1 \\ &- \alpha(\alpha^3 - 10\alpha) = 1 \\ &\frac{1}{\alpha} = \alpha^3 - 10\alpha \end{aligned}$$

Abbiamo quindi scritto un'espressione razionale nel campo $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ come polinomio in $\alpha = \sqrt{2} + \sqrt{3}$ a coefficienti razionali.

Il procedimento utilizzato in questo esempio è valido anche nel caso di espressioni razionali più complesse: per razionalizzare ad esempio $\dfrac{\sqrt{2}}{\sqrt{2}+\sqrt{3}}$ basta considerare che $\dfrac{\sqrt{2}}{\sqrt{2}+\sqrt{3}} = \sqrt{2}\dfrac{1}{\sqrt{2}+\sqrt{3}}$ e ripetere le operazioni viste.

Bibliografia

[1] Artin, M. *Algebra*, 1997, Bollati Boringhieri

[2] Cox, D. A. *Galois Theory*, 2004, Wiley-Interscience

[3] Jacobson, N. *Lectures in Abstract Algebra - vol III: Theory of Fields and Galois Theory*, 1975, Springer

[4] Milne, J.S. *Fields and Galois Theory*, Version 4.21, September 2008

[5] Zariski, O. - Samuel, P. *Commutative Algebra*, 1958, D. Van Nostrand Company