Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali

Corso di Laurea Triennale in Matematica

ESTENSIONI SEPARABILI DI CAMPI E TEOREMA DELL'ELEMENTO PRIMITIVO

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.
Mirella Manaresi

Presentata da:
Alberto Landuzzi

Sessione II
Anno Accademico 2011-2012

Ai miei genitori,
per l'opportunitá concessami.

Introduzione

In questa tesi vengono studiate le estensioni separabili di campi e dimostrato un importante risultato della teoria dei campi, il *Teorema dell'Elemento Primitivo*. La dissertazione sará supportata da molti esempi che illustreranno i risultati di volta in volta ottenuti.

Il capitolo 1 contiene una breve panoramica sulle nozioni di base della teoria dei campi: quella di estensione di campi, e i concetti di estensione algebrica ed estensione finita.

Nel capitolo 2 viene presa in esame la nozione di separabilitá. La prima parte sará dedicata ai polinomi separabili: verrá data la definizione e si forniranno criteri per determinare se un polinomio é, o non é, separabile. La seconda parte invece, tratterá le estensioni separabili ed il concetto di campo perfetto.

Nel capitolo 3 verrá enunciato il Teorema dell'Elemento Primitivo di cui verrá data una rigorosa dimostrazione sia nel caso finito che nel caso infinito. Per concludere verrá dimostrato un teorema, dovuto a Steinitz, che fornisce una caratterizzazione completa delle estensioni finite che ammettono elemento primitivo.

Indice

Capitolo 1

Richiami

Questo primo capitolo é una breve raccolta di nozioni utili per il seguito della trattazione.
Nella prima sezione si espongono i concetti di campo ed estensione di campi. Nella seconda sezione vengono invece definiti i concetti di estensione algebrica ed estensione finita.

1.1 Estensioni di campi

Definizione 1.1. Un anello K si dice *campo* se $K - \{0\}$ é un gruppo commutativo rispetto alla moltiplicazione, ovvero se ogni elemento non nullo dell'anello é invertibile. Un sottoinsieme non vuoto $S \subseteq K$ é un *sottocampo* se é un sottoanello ed eredita da K la struttura di campo. Si chiama *sottocampo fondamentale* o *campo primo* di K il piú piccolo campo contenuto in esso. Denotiamo con $K^\times := K - \{0\}$ il *gruppo moltiplicativo* del campo K.

Esempio 1.2. Gli insiemi numerici $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono campi, mentre $\mathbb{Z}$ non é un campo.

Definizione 1.3. Dato un dominio di integritá D, chiamiamo *campo dei quozienti* di D il campo $Q(D)$ i cui elementi sono della forma $\frac{a}{b}$ con $a, b \in D$, $b \neq 0$. Esso é il piú piccolo campo contenente D. Se K é un campo,

chiaramente il suo campo dei quoziente coincide con K stesso, ovvero $Q(K) = K$.

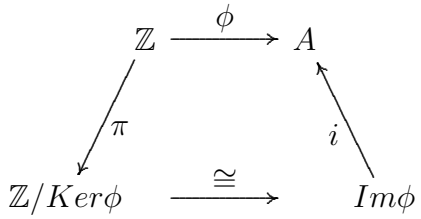
Definizione 1.4. Dato un anello A esiste un unico morfismo di anelli da $\mathbb{Z}$ ad A, ed é della forma:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow A \\ 1 &\longmapsto 1_A \\ n &\longmapsto n \cdot 1_A := \underbrace{1_A + \ldots + 1_A}_{n volte} \end{aligned}$$

$Im\phi$ si chiama *sottoanello fondamentale* di A. Chiamiamo *caratteristica* di A (e si indica con $carA$) l'ordine di 1_A nel gruppo $(A, +)$, cioé:

- $carA = n$ se $|1_A| = n$
- $carA = 0$ se $|1_A| = \infty$

Dal *Teorema Fondamentale di Omomorfismo per gli Anelli* segue che:



con $Ker\phi = \{n \in \mathbb{Z} \mid n \cdot 1_A = 0\} = \langle carA \rangle$. Si ha quindi:

- $carA = 0 \Leftrightarrow Ker\phi = \langle 0 \rangle \Leftrightarrow \mathbb{Z}/Ker\phi = \mathbb{Z} \Leftrightarrow Im\phi \cong \mathbb{Z}$
- $carA = n \Leftrightarrow Ker\phi = \langle n \rangle \Leftrightarrow \mathbb{Z}/Ker\phi = \mathbb{Z}_n \Leftrightarrow Im\phi \cong \mathbb{Z}_n$

Osservazione 1.5. Se K é un campo, allora $carK = 0$ oppure $carK = p$ con p primo. Inoltre se $carK = 0$ allora K ha sottocampo fondamentale isomorfo a $\mathbb{Q}$, mentre se $carK = p$ allora K ha sottocampo fondamentale isomorfo a $\mathbb{Z}_p$.

Dimostrazione. Se K é un campo allora é anche un dominio di integritá. Ponendo nella definizione sopra $A = K$ si ha che $Im\phi$ é un sottocampo di K, dunque anche $Im\phi$ é un dominio. Da ció segue che $Im\phi \cong \mathbb{Z}$ oppure $Im\phi \cong \mathbb{Z}_p$ con p primo. Se $Im\phi \cong \mathbb{Z}$ allora $carK = 0$ e K contiene un sottocampo isomorfo a $Q(\mathbb{Z}) = \mathbb{Q}$. Se invece $Im\phi \cong \mathbb{Z}_p$ si ragiona in modo analogo tenendo presente che $\mathbb{Z}_p$ é un campo e che il campo dei quozienti di un campo é il campo stesso. □

Definizione 1.6. Un campo L si dice *estensione* del campo K se esiste un'immersione di K in L. Identificando K con la sua immagine isomorfa in L, useremo come notazione L/K o anche $K \subseteq L$.

Esempio 1.7. Questi sono alcuni esempi di estensioni di campi:

1. Ogni campo K é estensione del suo sottocampo fondamentale. Precisamente K ha caratteristica zero se e solo se $\mathbb{Q} \subseteq K$ e K ha caratteristica positiva p se e solo se $\mathbb{F}_p \subseteq K$.

2. Sia $X = \{x_i\}_{i \in I}$ un insieme di indeterminate indipendenti. Se consideriamo $K(X)$ il campo delle funzioni razionali, avremo $K \subseteq K(X)$.

Definizione 1.8. Sia L/K una estensione di campi, e sia $\alpha \in L$. Si indica con $K(\alpha)$ il *sottocampo di L generato* da K e da α, e si ha che:

1. $K(\alpha) = \bigcap_i F_i$ con F_i sottocampi di L contenenti K ed α

2. $K(\alpha)$ é il piú piccolo sottocampo di L contenente K ed α

3. $K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)}$ con $f, g \in K[\alpha]$, $g \neq 0\}$

Una estensione di campi della forma $K \subseteq K(\alpha)$, ottenuta cioé aggiungendo un solo elemento, si dice *semplice*. In modo del tutto analogo si puó estendere un campo con un insieme finito di elementi come segue:

Definizione 1.9. Sia L/K una estensione di campi, e siano α_1,...,$\alpha_n \subseteq L$. si indica con $K(\alpha_1, ..., \alpha_n)$ il *sottocampo di L generato* da K e da α_1,...,α_n. Valgono le medesime proprietá enunciate nella precedente definizione.

Si puó anche vedere $K(\alpha_1, ..., \alpha_n)$ come campo ottenuto mediente le estensioni successive $K(\alpha_1)(\alpha_2)...(\alpha_n)$.

Obiettivo di questa tesi sará per l'appunto trovare le condizioni su α_1,...,α_n sufficienti ad assicurare che l'estensione $K(\alpha_1, ..., \alpha_n)$ sia semplice, ovvero che esista un elemento $\alpha \in L$ (detto *elemento primitivo*) tale che $K(\alpha_1, ..., \alpha_n) = K(\alpha)$.

1.2 Estensioni algebriche e finite

In questa sessione daremo una panoramica generale sulle nozioni di algebricitá e finitezza per estensioni di campi, vedremo come sono legate tra loro e forniremo alcuni esempi chiarificatori.

Definizione 1.10. Sia L/K una estensione di campi, allora L puó essere visto come K-spazio vettoriale con la moltiplicazione per scalari data da:

$$\begin{aligned} K \times L &\longrightarrow L \\ (k, l) &\longmapsto kl \end{aligned}$$

Chiamiamo *grado dell'estensione* L/K, e lo denotiamo con $[L : K]$, la $dim_k L$. Se $[L : K] < \infty$ diciamo che L/K é una estensione *finita* di campi.

Esempio 1.11. $\mathbb{C}/\mathbb{R}$ é una estensione finita con $[\mathbb{C} : \mathbb{R}] = 2$, e una $\mathbb{R}$-base di $\mathbb{C}$ é data da $\{1, i\}$.

Il seguente teorema mostra come si comporta la nozione di grado quando si hanno catene di estensioni successive:

Teorema 1.12 (Teorema della Torre)**.** *Siano $K \subseteq M \subseteq L$ estensioni di campi. Allora:*

$$L/K \text{ é finita} \iff L/M \text{ ed } M/K \text{ sono finite}$$

In questo caso si ha che $[L : K] = [L : M][M : L]$.

Dimostrazione. Siano $x_1, \dots, x_r$ una K-base di M e $y_1, \dots, y_s$ una M-base di L. Vogliamo mostrare che $\{x_i y_j\}$ sono una K-base di L, cioé che generano L e sono linearmente indipendenti. Sia $x \in L$, allora

$$\left.\begin{aligned} x &= \sum_{j=1}^{s} \alpha_j y_j \quad \text{con} \quad \alpha_j \in M \\ \alpha_j &= \sum_{i=1}^{r} a_{ij} x_i \quad \text{con} \quad a_{ij} \in K \end{aligned}\right\} \Rightarrow x = \textstyle\sum_{i,j} a_{ij} x_i y_j$$

cioé generano L come K-spazio vettoriale. Mostriamo che sono linearmente indipendenti: sia $\sum_{i,j} a_{ij} x_i y_j = 0$ una loro combinazione lineare nulla. Separando le sommatorie ottengo

$$\sum_{j=1}^{s} (\underbrace{\sum_{i=1}^{r} a_{ij} x_i}_{\in M}) y_j = 0$$

ma gli y_j sono una M-base di L, dunque $\sum_{i=1}^{r} a_{ij} x_i = 0 \quad \forall j$, ma siccome gli x_i sono una K-base di M segue che $a_{ij} = 0 \quad \forall i, j$. □

Definizione 1.13. Sia $K \subseteq L$ una estensione di campi, e sia $\alpha \in L$. Allora α si dice *algebrico* su K se esiste un polinomio non costante $f \in K[x]$ tale che $f(\alpha) = 0$. In caso contrario α si dice *trascendente*. Se α é algebrico si chiama *polinomio minimo* di α l'unico polinomio $p_\alpha \in K[x]$ non costante, monico, ed irriducibile su K, che si annulla in α.

Osservazione 1.14. Consideriamo $K \subseteq L$ campi, $\alpha \in L$ elemento algebrico su K, e sia p il suo polinomio minimo. Allora L contiene un sottocampo $K(\alpha) \cong K[x]/\langle p \rangle$, e tale $K(\alpha)$ é il piú piccolo sottocampo di L contenente K e α. Inoltre se n é il grado del polinomio minimo p, vale che $1, \alpha, \dots, \alpha^{n-1}$ é una base per $K(\alpha)$ su K e $[K(\alpha) : K] = n$. Possiamo quindi identificare le estensioni di campi con un elemento algebrico definite in 1.8 come quozienti dell'anello $K[x]$ mediante l'ideale generato dal polinomio minimo di quell'elemento. Vediamo un esempio pratico:

Esempio 1.15. Consideriamo $\mathbb{Q} \subseteq \mathbb{R}$ e $\sqrt{2} \in \mathbb{R}$. $p = x^2 - 2$ é il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$. Allora avremo che:

- $\sqrt{2}$ é algebrico su $\mathbb{Q}$
- $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle$
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ e $\{1, \sqrt{2}\}$ é una base su $\mathbb{Q}$

Definizione 1.16. Una estensione di campi $K \subseteq L$ si dice *algebrica* se ogni elemento di L é algebrico su K.

Vediamo ora come una estensione di campi finita sia anche algebrica, e mostreremo con un esempio come non valga il viceversa:

Teorema 1.17. *Sia L/K estensione di campi. Allora L/K é finita se e solo se L/K é algebrica ed L é finitamente generato su K.*

Dimostrazione. Mostriamo prima la necessitá. Sia quindi $[L : K] = n$ e sia $x_1, \ldots, x_n$ una base di L su K. Poiché é base riesco a generare tutto L, quindi $L = K(x_1, \ldots, x_n)$. Sia ora $l \in L$ e considero gli $n+1$ elementi $1, l, l^2, \ldots, l^n$. Essi sono necessariamente linearmente dipendenti, quindi $\exists\ a_0, a_1, \ldots, a_n \in K$ tali che $a_o + a_1 l + \ldots + a_n l^n = 0$. Allora l é algebrico su K e, data l'arbitrarietá di l, si conclude.
Viceversa, sia L finitamente generato, cioé $L = K(x_1, \ldots, x_n)$. Dal Teorema 1.12 si ha che:

$$[L : K] = [K(x_1, \ldots, x_n) : K(x_1, \ldots, x_{n-1})] \cdot \ldots \cdot [K(x_1) : K] < \infty$$

in quanto ogni x_i, essenso per ipotesi algebrico su K, lo é certamente su una estensione di quest'ultimo, quindi ogni fattore che compare nel prodotto é finito. □

Questo teorema mostra che un'estensione algebrica non é necessariamente finita se manca l'ipotesi che sia finitamente generata:

Esempio 1.18. Un campo K si dice *algebricamente chiuso* se ogni polinomio $f \in K[x]$ di grado positivo ha almeno una radice in K. Dato un campo K la sua *chiusura algebrica* é un campo algebricamente chiuso $\overline{K}$ con $K \subseteq \overline{K}$ e tale che l'estensione $\overline{K}/K$ sia algebrica.
Se consideriamo l'insieme $\overline{\mathbb{Q}}$ di tutti i numeri complessi che sono algebrici su $\mathbb{Q}$, si ha che $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ é per definizione algebrica, ma chiaramente infinita. Infatti se l'estensione fosse finita, posto $n = [\overline{\mathbb{Q}} : \mathbb{Q}]$, dal Teorema della Torre seguirebbe che ogni elemento di $\overline{\mathbb{Q}}$ dovrebbe avere grado che divide n. Ma presi $m > n$ e p primo, il criterio di Eisenstein mi dice che il polinomio $x^m - p$ é irriducibile su $\mathbb{Q}$, da cui l'assurdo.

Capitolo 2

Separabilitá

2.1 Polinomi separabili

Definizione 2.1. Sia K un campo, e sia $f \in K[x]$ un polinomio non costante. Un *campo di spezzamento* (abbreviato con *c.s.*) di f su K é una estensione di campi $K \subseteq L$ tale che:

1. $f = c(x-\alpha_1)^{s_1} \cdot \ldots \cdot (x-\alpha_n)^{s_n}$ con $c \in K$, $\alpha_i \in L$, $s_i \in \mathbb{N} - \{0\}$
2. $L = K(\alpha_1, \ldots, \alpha_n)$

Osservazione 2.2. Un importante teorema che in questa sede non dimostriamo ([2], Teoremi 5.1.5. e 5.1.6., pag. 102-105), ci assicura che, dato un qualsiasi polinomio f a coefficienti nel campo K, esso ammette sempre un campo di spezzamento che é unico a meno di isomorfismi. Quindi negli enunciati che seguiranno possiamo parlare di "polinomi che nel loro campo di spezzamento...".

Dalla definizione 2.1 abbiamo visto come un polinomio nel suo c.s. si decomponga nel prodotto di fattori lineari $f = c(x-\alpha_1)^{s_1} \cdot \ldots \cdot (x-\alpha_n)^{s_n}$ dove le α_i sono le *radici* del polinomio e le s_i le rispettive *molteplicitá*. Diciamo che α_i é *radice multipla* se $s_i > 1$, *radice semplice* se $s_i = 1$.

Teorema 2.3. *Sia $f \in K[x]$, f' la sua derivata e sia α radice di f. Allora:*

$$\alpha \text{ é radice multipla di } f \iff f'(\alpha) = 0$$

Dimostrazione. Sia $f = (x-\alpha)^s)g$ con $g \in K[x]$ t.c. $g(\alpha) \neq 0$.
Derivando otteniamo:
$f' = n(x-\alpha)^{n-1}g + (x-\alpha)^n g' = (x-\alpha)h$ con $h \in K[x]$, quindi f' si annulla in α. Viceversa $f = (x-\alpha)h$ e $f' = h + (x-\alpha)h'$ con $h \in K[x]$. Ma per ipotesi $f'(\alpha) = 0$, quindi $h(\alpha) = 0$, cioé $h = (x-\alpha)g$. Sostituendo trovo che $f = (x-\alpha)^2 g$, cioé che la molteplicitá di α é almeno 2. □

Definizione 2.4. Un polinomio $f \in K[x]$ si dice *separabile* se nel suo campo di spezzamento non ha radici multiple.

Esempio 2.5.

1. In $\mathbb{R}[x]$ i polinomi $x^2 - x$ e $x^3 - 2$ sono separabili: il primo ha 2 radici distinte su $\mathbb{R}$, cioé 0 ed 1, mentre il secondo ha 3 radici distinte su $\mathbb{C}$, precisamente $\sqrt[3]{2}$, $w\sqrt[3]{2}$, $w^2\sqrt[3]{2}$ con $w = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ radice cubica dell'unitá.

2. Consideriamo ora $X^3 - 2 \in \mathbb{F}_3[x]$. Esso é inseparabile perché (ricordiamoci che in $\mathbb{F}_3$ vale $-2 = 1$) si ha $x^3 - 2 = x^3 + 1 = (x+1)^3$, cioé ha una sola radice di molteplicitá 3.

Definizione 2.6. Sia α algebrico su K. Si dice che α é *separabile su K* se il suo polinomio minimo in $K[x]$ é separabile. In caso contrario α si dice *inseparabile su K*.

Esempio 2.7. I numeri reali $\sqrt{2}$ e $\sqrt{3}$ sono entrambi separabili su $\mathbb{Q}$, infatti i loro rispettivi polinomi minimi $x^2 - 2$ e $x^2 - 3$ sono separabili. Per esempio $x^2 - 2$ spezza in $\mathbb{Q}(\sqrt{2})$ come $(x - \sqrt{2})(x + \sqrt{2})$.

Abbiamo detto che per vedere se un polinomio é separabile oppure no dobbiamo guardare come esso si spezza nel suo c.s., tuttavia determinare il c.s. di un polinomio e la sua fattorizzazione non é quasi mai di facile esecuzione. Spostiamo quindi il problema su un altro versante, ovvero determiniamo la presenza o meno di radici multiple (e quindi la separabilitá) in

base al "comportamento" del nostro polinomio rispetto alla sua derivata.

Dato un polinomio non costante f, quando $f = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, si definisce *discriminante* di f

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Ricordiamo che per i polinomi vale l'identitá di Bezout, la quale dice che presi $f, g \in K[x]$ con $(f, g) = 1$ (cioé primi tra loro), allora esistono $u, v \in K[x]$ tali che $fu + gv = 1$.

Teorema 2.8. *Se $f \in K[x]$ é un polinomio monico e non costante,allora sono equivalenti i seguenti:*

1. *f é separabile.*
2. *$\Delta(f) \neq 0$.*
3. *$(f, f') = 1$.*

Dimostrazione. Se f ha grado 1 allora non c'é niente da dimostrare, quindi possiamo assumure che f abbia grado > 1.
Se $\alpha_1, \ldots, \alpha_n$ sono tutte le radici di f nel suo c.s., allora la formula del discriminante mostra chiaramente che dire $\Delta(f) \neq 0$ equivale a dire che $\alpha_i \neq \alpha_j$ per ogni $i < j$. Quindi l'equivalenza di 1) e 2) risulta provata. Resta da vedere 1) $\Leftrightarrow$ 3): sia f separabile e sia α una sua radice in una qualche estensione di K. Allora posso scrivere $f = (x - \alpha)h$ con $h(\alpha) \neq 0$ e $f' = h + (x - \alpha)h'$. Poiché $f'(\alpha) = h(\alpha) \neq 0$, α non é radice di f'. Ne risulta che f ed f' non hanno radici comuni e quindi nemmeno fattori comuni in $K[x]$, perció $(f, f') = 1$. Viceversa, se $(f, f') = 1$ allora ogni radice di f non puó essere allo stesso tempo radice di f', e quindi in virtú del Teorema 2.3 é radice semplice di f. Quindi f é separabile. □

Esempio 2.9. 1. Prendiamo il polinomio $f = x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 2 \in \mathbb{F}_3$ e calcoliamo:

$$f' = (2x^2 + 2)(x^2 + 2x + 2)$$

$$f = (2x^2 + 2)(2x^4 + 2x^3 + 2x + 1)$$

quindi $(f, f') \neq 1$ perché sicuramente $(2x^2 + 2) \mid (f, f')$, perció il polinomio f non é separabile. Infatti $f = (x^2 + 1)^2(x^2 + x + 2)$. Notare come siamo stati in grado di vedere se f é separabile o meno senza averne precedentemente dato la fattorizzazione.

2. Consideriamo il polinomio $f = x^n - a \in K[x]$, con $a \in K^*$. Il teorema dice che f é separabile se e solo se é coprimo con la sua derivata che é $f' = nx^{n-1}$. In ogni caso abbiamo che:

   - Se $n \neq 0$ in K, allora l'unico fattore irriducibile di f' é x, che chiaramente non divide f. Quindi in questo caso f e f' sono coprimi.
   - se $n = 0$ in K, allora $f' = 0$ e $f \mid f'$. Quindi in questo caso f e f' non sono coprimi.

   Ne segue che $x^n - a$ é separabile se e solo se $n \neq 0$ in K (che equivale a dire $p \nmid n$ quando K ha caratteristica p).

Corollario 2.10. *Sia $f \in K[x]$ separabile e sia $K \subseteq L$, allora ogni fattore di f su $L[x]$ é separabile.*

Dimostrazione. sia g un fattore di f, quindi $f = gh$ in $L[x]$. Poiché f é separabile il Teorema 2.8 e l'identita di Bezout mi dicono che:

$$1 = fu + f'v = ghu + (g'h + gh')v = g(hu + h'v) + g'(hv)$$

quindi $(g, g') = 1$, cioé g é separabile. □

Per quanto riguarda polinomi *irriducibili*, possiamo raffinare il Teorema 2.8 per ottenere un modo piú semplice per testare la separabilitá di un polinomio rispetto allo studio della sua derivata.

Teorema 2.11. *Sia K un campo, un polinomio f irriducibile in $K[x]$ é separabile se e solo se $f' \neq 0$. In particolare:*

se $carK = 0$ ogni polinomio irriducibile é separabile.

se $carK = p$ un polinomio irriducibile é separabile se e solo se non é un polinomio in x^p.

Dimostrazione. Sia f un polinomio irriducibile in $K[x]$. Dal Teorema 2.8 la separabilitá é equivalente a dire che $(f, f') = 1$. Se $(f, f') \neq 1$, allora $f \mid f'$ poiché f é irriducibile, e questo é possibile se e solo se $f' = 0$ avendo f' grado piú basso di f. Quindi $(f, f') = 1$ (cioé f separabile) se e solo se $f' \neq 0$. In caratteristica 0 un polinomio f irriducibile é sicuramente non costante, avrá perció derivata non nulla, e per quanto appena visto é separabile. Sia ora K con caratteristica p, e sia $f = a_0 + a_{k_1}x^{k_1} + \ldots + a_{k_n}x^{k_n}$ con $a_{k_i} \neq 0$ per ogni $i = 1, ..., n$. Allora $f' = 0$ se e solo se p divide tutti i coefficienti $k_i a_{k_i}$ di f'. Poiché abbiamo supposto ($a_{k_i} \neq 0$) che $p \nmid a_{k_i}$, allora $p \mid k_i$ per ogni $i = 1, ..., n$. Quindi $k_i = ps_i$ e $f = a_0 + a_{k_1}x^{ps_1} + \ldots + a_{k_n}x^{ps_n} = c_0 + c_1x^p + \ldots + c_rx^{pr} =: g(x^p)$, con $r = s_n$. Perció f é separabile se e solo se questo non accade. □

Esempio 2.12.

1. In $\mathbb{Q}[x]$ ogni polinomio irriducibile é separabile.
2. Prendiamo $K = \mathbb{F}_p(u)$ il campo delle funzioni razionali su $\mathbb{F}_p$. Il polinomio $f = x^p - u \in K[x]$ é irriducibile (per Eisenstein rispetto ad u). Poiché $(x^p - u)' = 0$ il Teorema 2.11 dice che $x^p - u$ é inseparabile. Ma potevamo vedere tutto ció anche direttamente, se infatti consideriamo una radice α del polinomio in un campo piú grande, avremo $\alpha^p = u$, e quindi $x^p - u = x^p - \alpha^p = (x - \alpha)^p$. Cioé nel suo campo di spezzamento L ha un'unica radice di moltelicitá p. Inoltre $L = K(\alpha)$ ed, essendo f il polinomio minimo di α, si ha che $[L : K] = p$.

2.2 Estensioni separabili

Abbiamo visto cosa vuol dire essere separabile per un polinomio o per un elemento del campo. Vediamo ora cosa vuol dire essere separabile per una

estensione di campi:

Definizione 2.13. Un'estensione algebrica di campi L/K si dice *separabile* se ogni elemento di L é separabile su K. Il campo K si dice *perfetto* se ogni sua estensione algebrica é separabile.

La seguente proposizione discende direttamente dalle definizioni:

Proposizione 2.14. *Per un campo K le seguenti proprietá sono equivalenti:*

1. *K é perfetto;*
2. *Ogni polinomio irriducibile di $K[x]$ é separabile su K;*
3. *Ogni $\alpha \in \overline{K}$ é separabile su K;*
4. *$\overline{K}$ é un ampliamento separabile di K.*

Definiamo ora un'applicazione di notevole importanza per i campi di caratteristica positiva p, e grazie alla quale saremo in grado di dimostrare due importanti risultati sulla separabilitá dei campi finiti.

Definizione 2.15. Sia K un campo di caratteristica positiva p. Si definisce *omomorfismo di Fröbenius* il seguente omomorfismo di campi:

$$\begin{aligned} \phi : K &\to K \\ a &\mapsto a^p. \end{aligned}$$

Come ogni omomorfismo di campi il *Fröbenius* é iniettivo.

In modo analogo a quanto fatto per la separabilitá, vediamo con la seguente Proposizione come la caratteristica di un campo mi permetta di determinare con facilitá se esso sia perfetto o meno.

Proposizione 2.16. *Sia K un campo. Allora:*

- *Se K ha caratteristica 0, allora K é perfetto.*

- *Se K ha caratteristica p, con p primo, le seguenti affermazioni sono equivalenti:*

  1. *K é perfetto;*
  2. *Per ogni $a \in K$, il polinomio $x^p - a$ ha una radice in K;*
  3. *Ogni elemento $a \in K$ é una potenza p-esima;*
  4. *Il Fröbenius é suriettivo;*
  5. *Il Fröbenius é un automorfismo.*

Dimostrazione. Se il campo K ha caratteristica 0 abbiamo visto che ogni polinomio irriducibile é separabile, dunque per la Proposizione 2.14 é perfetto. Supponiamo quindi che K abbia caratteristica p. 1) $\Rightarrow$ 2) perché se per un qualche $a \in K$ il polinomio $x^p - a$ non avesse radici, allora sarebbe irriducibile e, per il Teorema 2.11, separabile, quindi K non sarebbe perfetto. L'equivalenza di 2), 3), 4) é evidente, cosí come quella di 4) e 5) perché ogni omomorfismo di campi é iniettivo. Vediamo che 3) $\Rightarrow$ 1) e abbiamo concluso: Supponiamo che ogni elemento di K sia una potenza p-esima e sia $f \in K[x]$ irriducibile su K. Se f non fosse separabile su K, allora per il Teorema 2.11 si avrebbe $f = c_0 + c_1 x^p + \ldots + c_r x^{pr}$, con $r \geq 0$. Posto $c_i := a_i^p$ avrei:

$$f = a_0^p + a_1^p x^p + \ldots + a_r^p x^{pr} = (a_0 + a_1 x + \ldots + a_r x^r)^p$$

e questa é una contraddizione perché avevamo supposto f irriducibile su K. Dunque f é separabile e, per la Proposizione 2.14, K é perfetto. □

Corollario 2.17. *Ogni campo finito é perfetto.*

Dimostrazione. Un campo finito ha necessariamente caratteristica p, con p primo. Il Fröbenius é iniettivo perché omomorfismo di campi, e poiché é iniettivo su di un campo finito allora é anche suriettivo: quindi é un automorfismo. Per la Proposizione 2.16 il campo é perfetto. □

Esempio 2.18. 1. Per ogni primo p, il campo $\mathbb{F}_p$ é perfetto.

2. Se consideriamo $\mathbb{F}_p(u)$ il campo delle funzioni razionali su $\mathbb{F}_p$ come nell'esempio 2.12, abbiamo visto che il polinomio $x^p - u$ é irriducibile ma non é separabile. Quindi $\mathbb{F}_p(u)$ non é perfetto.

Capitolo 3

Teorema dell'Elemento Primitivo

Se L/K é una estensione finita di campi e, per un certo $\alpha \in L$, risulta che $L = K(\alpha)$, l'elemento α si chiama *elemento primitivo di L su K*. Per questo motivo il Teorema che esamineremo in questo capitolo prende il nome di *Teorema dell'Elemento Primitivo*. Non tutte le estensioni finite peró ammettono elemento primitivo, condizione essenziale come vedremo é che l'estensione sia anche separabile. Mostreremo inoltre che non vale il viceversa, fornendo un esempio di estensione semplice (ottenuta mediante un elemento primitivo) che é finita ma non separabile.

Esistono varie formulazioni di questo importante risultato della teoria dei campi, noi ci atterremo alla formulazione classica.

Teorema 3.1 (Teorema dell'Elemento Primitivo)**.** *Sia $K \subset L = K(\alpha_1, \ldots, \alpha_n)$ una estensione di campi finita, dove ogni α_i é separabile su K. Allora esiste $\alpha \in L$ separabile su K tale che $L = K(\alpha)$.*
Inoltre, se K é infinito, α puó essere scelto della forma

$$\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n$$

con $t_1, \ldots, t_n \in K$.

La dimostrazione di questo teorema si diversifica notevolmente a seconda che il campo K sia finito o infinito (attenzione: non si parla di caratteristica). Quindi tratteremo separatamente i due casi.

Cominciamo con la dimostrazione nel caso di campo infinito:

Dimostrazione. (Caso K infinito). Supponiamo che K sia infinito e che $L = K(\alpha_1, \ldots, \alpha_n)$, dove ogni α_i é separabile su K. Useremo l'induzione su n per mostrare che esistono $t_1, \ldots, t_n \in K$ tali che $L = K(t_1\alpha_1 + \ldots + t_n\alpha_n)$ e $t_1\alpha_1 + \ldots + t_n\alpha_n$ é separabile su K (questo é proprio il nostro α).

Nel caso in cui $n = 1$ non cé nulla da dimostrare. Sia quindi $n = 2$ e $L = K(\beta, \gamma)$. Siano $f, g \in K[x]$ i polinomi minimi rispettivamente di β, γ, e di grado rispettivamente l ed m. Se consideriamo il campo di spezzamento di fg, poiché per ipotesi β, γ sono separabili (e quindi hanno polinomio minimo separabile) si avrá che:

$$f \quad \text{ha radici distinte} \quad \beta = \beta_1, \beta_2, \ldots, \beta_l,$$

$$g \quad \text{ha radici distinte} \quad \gamma = \gamma_1, \gamma_2, \ldots, \gamma_m.$$

Poiché K é infinito per ipotesi, esisterá di certo un $\lambda \in K$ tale che

$$\lambda \neq \frac{\beta_i - \beta_r}{\gamma_s - \gamma_j} \quad \text{per} \quad 1 \leq r, i \leq l,\ 1 \leq s, j \leq m,\ s \neq j. \tag{3.1}$$

da cui si ricava facilmente che

$$\beta_r + \lambda\gamma_s \neq \beta_i + \lambda\gamma_j \quad \text{per} \quad (r, s) \neq (i, j). \tag{3.2}$$

In particolare, avendo posto $\beta = \beta_1$ e $\gamma = \gamma_1$, si ha che

$$\beta + \lambda\gamma \neq \beta_i + \lambda\gamma_j \quad \text{per} \quad 1 \leq i \leq l,\ 2 \leq j \leq m. \tag{3.3}$$

Proviamo a questo punto che $K(\beta + \lambda\gamma) = K(\beta, \gamma)$. Poiché l'inclusione $K(\beta + \lambda\gamma) \subset K(\beta, \gamma)$ é ovvia, é sufficiente mostrare che $\beta, \gamma \in K(\beta + \lambda\gamma)$ per provare l'inclusione opposta. Studiamo quindi γ. Osserviamo che:

- γ é radice di $g(x)$ e $g \in K[x] \subset K(\beta + \lambda\gamma)[x]$;

- γ é radice di $f(\beta + \lambda\gamma - \lambda x)$ che é un polinomio di $K(\beta + \lambda\gamma)[x]$.

Il nostro obbiettivo sará studiare il massimo comune divisore tra questi due polinomi. Notiamo che se il massimo comune divisore fosse 1, dall'identitá di Bezout si avrebbe che:

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

per qualche $A, B \in K(\beta + \lambda\gamma)[x]$, e ció non é possibile in quanto calcolando questa uguaglianza in $x = \gamma$ si avrebbe $0 = 1$. Quindi

$$h(x) = (g(x), f(\beta + \lambda\gamma - \lambda x)) \in K(\beta + \lambda\gamma)[x]$$

ha grado ≥ 1. Ma se il grado fosse > 1, poiché $h(x) \mid g(x)$ vorrebbe dire che γ_j é radice di $h(x)$ per qualche $2 \leq j \leq m$. Ma siccome $h(x) \mid f(\beta+\lambda\gamma-\lambda x)$, γ_j dovrebbe essere anche radice di quest'ultimo, cioé $f(\beta + \lambda\gamma - \lambda\gamma_j) = 0$. Siccome le radici di f sono $\beta = \beta_1, \beta_2, \ldots, \beta_l$, questo implica che

$$\beta + \lambda\gamma - \lambda\gamma_j = \beta_i \quad \text{per qualche} \quad 1 \leq i \leq l,$$

e ció contraddice 3.3. Quindi h ha grado 1, ed essendo γ una sua radice, é della forma $h = x - \gamma$. Inoltre $h \in K(\beta + \lambda\gamma)[x]$, quindi $\gamma \in K(\beta + \lambda\gamma)$. Ma $\beta = (\beta + \lambda\gamma) - \lambda \cdot \gamma$, cioé β é una combinazione di elementi di $K(\beta + \lambda\gamma)$ con $\lambda \in K$, quindi anche $\beta \in K(\beta + \lambda\gamma)$. Ho perció dimostrato che $K(\beta, \gamma) = K(\beta + \lambda\gamma)$.
Sia ora $p \in K[x]$ il polinomio minimo di $\beta + \lambda\gamma$ su K. Per mostrare che $\beta + \lambda\gamma$ é separabile (é il nostro elemento primitivo) dobbiamo far vedere che p é separabile. A questo scopo consideriamo il polinomio

$$s(x) = \prod_{j=1}^{m} f(x - \lambda\gamma_j). \tag{3.4}$$

Essendo $\gamma = \gamma_1$ e valutando $s(x)$ in $\beta + \lambda\gamma$ risulta che

$$\begin{aligned} s(\beta+\lambda\gamma) &= \prod_{j=1}^{m} f(\beta+\lambda\gamma-\lambda\gamma_j) = \\ &= f(\beta+\lambda\gamma-\lambda\gamma_1)\prod_{j=2}^{m} f(x-\lambda\gamma_j) = \\ &= f(\beta+\lambda\gamma-\lambda\gamma)\prod_{j=2}^{m} f(x-\lambda\gamma_j) = \\ &= f(\beta)\prod_{j=2}^{m} f(x-\lambda\gamma_j) = \\ &= 0 \end{aligned}$$

poiché β era radice di f. quindi $\beta + \lambda\gamma$ é radice di s. Ma non solo, vale che $s \in K[x]$. Infatti si verifica facilmente che una permutazione delle γ_j lascia invariato s, cioé s é un polinomio simmetrico. Tenendo a mente che $f \in K[x]$, le γ_j sono le radici di $g \in K[x]$ e che $\lambda \in K$, per il *Teorema Fondamentale sui Polinomi Simmetrici* ([1] Teorema 2.7.7, pag. 81) risulta che i coefficienti di s sono dati dalle funzioni simmetriche elementari fino all'ordine ordine m calcolate nelle $\lambda\gamma_j$. Per quanto detto ne segue che s é a coefficienti in K.
Ne segue che, essendo $\beta + \lambda\gamma$ radice sia di p che di s, ed essendo p il suo polinomio minimo, necessariamente $p \mid s$ in $K[x]$.
Inoltre dalla fattorizzazione di f si ha che

$$f = (x-\beta_1)\cdot\ldots\cdot(x-\beta_l) = \prod_{i=1}^{l}(x-\beta_i)$$

e sostituendo nell'espressione di s si trova che

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

Dalla fattorizzazione di s appena trovata e da 3.2 si deduce che s ha tutte radici distinte, e cosí pure p che divide s. Quindi p é separabile, e per

definizione $\beta + \lambda\gamma$ é separabile su K. Ponendo poi $t_1 = 1$ e $t_2 = \lambda$, il teorema risulta dimostrato per $n = 2$.
Supponiamo ora che $n > 2$ e che $L = K(\alpha_1, \ldots, \alpha_n)$, dove ogni α_i é separabile su K. Supponiamo che il teorema valga per $n - 1$. Per ipotesi induttiva esistono $t_1, \ldots, t_{n-1} \in K$ tali che $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha_0)$, con $\alpha_0 = t_1\alpha_1 + \ldots + t_{n-1}\alpha_{n-1}$ separabile su K.
Allora

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_0)(\alpha_n) = K(\alpha_0, \alpha_n).$$

Ma abbiamo appena visto che il teorema vale per $n = 2$ e si aveva $K(\alpha_0, \alpha_n) = K(\alpha_0 + \lambda\alpha_n)$ per un qualche $\lambda \in K$, con $\alpha_0 + \lambda\alpha_n$ separabile su K. Ponendo $t_n = \lambda$, allora

$$\alpha_0 + \lambda\alpha_n = t_1\alpha_1 + \ldots + t_n\alpha_n = \alpha$$

é l'elemento primitivo che stavamo cercando.
Ció conclude la dimostrazione del teorema nel caso di K infinito. □

Esempio 3.2. 1. Consideriamo l'estensione di campi $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Seguendo passo per passo la dimostrazione del Teorema, poniamo $\beta_1 = \sqrt{2}$, $\beta_2 = -\sqrt{2}$ con polinomio minimo $f = x^2 - 2$, e $\gamma_1 = \sqrt{3}$, $\gamma_2 = -\sqrt{3}$ con polinomio minimo $g = x^2 - 3$. Si verifica immediatamente che ogni $\lambda \neq 0 \in \mathbb{Q}$ soddisfa la 3.1, infatti sostituendo nel secondo membro di 3.1 i nostri valori di β_i e γ_j si ottiene:

$$\lambda = 0 \in \mathbb{Q}$$

oppure

$$\lambda = \pm\frac{\sqrt{2}}{\sqrt{3}} \notin \mathbb{Q}.$$

Quindi $\forall\ \lambda \in \mathbb{Q} - \{0\}$, $\sqrt{2} + \lambda\sqrt{3}$ é un elemento primitivo di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Prendendo per esempio $\lambda = 1$ si ottiene il risultato ben noto che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

2. Consideriamo l'estensione di campi $\mathbb{Q}(i, \sqrt[3]{2})/\mathbb{Q}$. Il polinomio minimo di i su $\mathbb{Q}$ é $f = x^2 + 1$, con radici distinte $\beta_1 = i$ e $\beta_2 = -i$. Il polinomio minimo di $\sqrt[3]{2})$ su $\mathbb{Q}$ é $g = x^3 - 2$, con radici distinte $\gamma_1 = \sqrt[3]{2}$, $\gamma_2 = w\sqrt[3]{2}$, $\gamma_3 = w^2\sqrt[3]{2}$, dove $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ é una radice cubica dell'unitá complessa. In modo analogo a prima, i valori di λ da scartare sono:

$$\lambda = 0 \in \mathbb{Q}$$

oppure

$$\lambda = \pm\frac{\sqrt[3]{2}(\frac{3}{2} \pm i\frac{\sqrt{3}}{2})}{2i} \notin \mathbb{Q} \quad \text{o} \quad \pm\frac{i\sqrt[3]{2}\sqrt{3}}{2i} \notin \mathbb{Q}.$$

Quindi, come prima, $\forall\ \lambda \in \mathbb{Q} - \{0\}$, $i + \lambda\sqrt[3]{2}$ é un elemento primitivo di $\mathbb{Q}(i, \sqrt[3]{2})$.

La dimostrazione del teorema nel caso di campo finito discende direttamente dal seguente risultato sui campi finiti:

Proposizione 3.3. *Il gruppo moltiplicativo $K^\times$ di un campo finito K é ciclico.*

Dimostrazione. Poniamo $|K^\times| = l$. Dobbiamo provare che in $K^\times$ esiste un elemento di periodo l (che sará il generatore di $K^\times$).
A tale scopo, sia m il minimo comune multiplo dei periodi degli elementi di $K^\times$. Vogliamo provare che $m = l$. Il teorema di Fermat ci dice che $a^l = 1$ per ogni $a \in K^\times$, quindi l é multiplo del periodo di ogni elemento di $K^\times$. Da cui

$$m \mid l.$$

Inoltre l'equazione $x^m - 1$ ha come soluzione tutti gli elementi di $K^\times$, ma allo stesso tempo ha al piú m soluzioni, quindi

$$l \leq m.$$

Ne segue che $m = l$.
L'esistenza del generatore cercato e quindi la conclusione della dimostrazione é conseguenza del lemma seguente. □

Lemma 3.4. *Sia G un gruppo commutativo. Se $a_1, \ldots, a_h$ sono elementi di G di periodo rispettivamente $n_1, \ldots, n_h$ ed $m = m.c.m.(a_1, \ldots, a_h)$, allora esiste un elemento $b \in G$ di periodo esattamente m.*

Dimostrazione. Si veda [3], Lemma pag 144. □

La dimostrazione del Teorema 3.1 nel caso di campo finito é ora immediata.

Dimostrazione. (Caso K finito). Se K é un campo finito, anche L, avendo grado finito su K, lo é. Dalla Proposizione 3.3 appena dimostrata segue immediatamente che $L^\times$ é un gruppo ciclico. Sia α un suo generatore, cioé $L^\times = \langle\alpha\rangle$. Pioché L contiene sia K che α l'inclusione $K(\alpha) \subseteq L$ é banale in quanto $K(\alpha)$ é il piú piccolo campo con tale proprietá. Ma vale di piú, siccome $K(\alpha)$ contiene tutte le potenze di α, sicuramente conterrá tutti gli elementi di $L^\times$ e contiene lo 0 in quanto campo: quindi vale $L \subseteq K(\alpha)$. Considerando le due inclusioni si ottiene quello che volevamo, cioé che

$$L = K(\alpha).$$

Mostriamo ora che α é separabile. Sia $q = |L^\times|$. Poiché $L^\times$ é ciclico di ordine q vale

$$(\alpha^i)^q = 1 \quad i = 1, \ldots, q-1$$

con α^i i distinti elementi di $L^\times$, da cui

$$(\alpha^i)^q - 1 = 0 \quad i = 1, \ldots, q-1$$

ovvero ogni α^i é radice di $x^q - 1 \in K[x]$. Poiché $x^q - 1$ ha al massimo q radici, si conclude che α^i sono tutte e sole le sue radici e sono distinte, cioé

$$x^q - 1 = (x-1)(x-\alpha)(x-\alpha^2) \cdot \ldots \cdot (x-\alpha^{q-1})$$

e quindi α é separabile perché il suo polinomio minimo é separabile. □

Mostriamo ora alcune dirette conseguenze dell'importante Teorema appena dimostrato.

Corollario 3.5. *Sia L/K una estensione finita.*

1. *Se L/K é separabile, allora esiste $\alpha \in L$ tale che $L = K(\alpha)$.*
2. *Se K ha caratteristica 0, allora esiste $\alpha \in L$ tale che $L = K(\alpha)$. Inoltre, se $L = K(\alpha_1, \ldots, \alpha_n)$, allora α puó essere preso della forma*

$$\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n$$

dove $t_1, \ldots, t_n \in K$.

Dimostrazione. Poiché L/K é finita sappiamo che possiamo scrivere $L = K(\alpha_1, \ldots, \alpha_n)$. Per quanto riguarda la parte 1), poiché l'estensione é per ipotesi separabile, ogni α_i é separabile, quindi basta applicare il Teorema 3.1. Dimostriamo ora la parte 2), sia quindi K di caratteristica 0. Allora K é necessariamente infinito perché contiene un sottocampo isomorfo a $\mathbb{Q}$, e per il Teorema 2.11 ogni α_i é separabile in quanto ha polinomio minimo separabile. Di nuovo, basta applicare il Teorema 3.1 nel caso di campo infinito e si conclude.

□

All'inizio del capitolo avevamo detto che non tutte le estensioni finite ammettono elemento primitivo. Il Corollario 3.5 ci dice che tale estensione non puó avere caratteristica 0, perché in quel caso l'estensione sarebbe automaticamente semplice.
Il seguente esempio in caratteristica p mostra una estensione finita che non ammette elemento primitivo:

Esempio 3.6. Richiamiamo alla mente l'esempio 2.12 e i risultati ottenuti. Sia $\mathbb{F}_p$ un campo di caratteristica p e siano u, t variabili. Consideriamo l'estensione di campi

$$K = \mathbb{F}_p(u, t) \subset L, \tag{3.5}$$

dove L é il campo di spezzamento di $(x^p - u)(x^p - t) \in K[x]$. Cosí esistono $\alpha, \beta \in L$ con $\alpha^p = u$ e $\beta^p = t$. Quindi possiamo ottenere L mediante due estensioni successive $L = K(\alpha)(\beta) = K(\alpha, \beta)$. Applicando il Teorema 1.12 si ottiene che $[L : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] = p \cdot p = p^2$, quindi L/K é un'estensione finita.
Mostriamo che 3.5 non ha elemento primitivo. Sia $\gamma \in L$, possiamo scriverlo come K-combinazione lineare degli elementi della base di L, cioe

$$\gamma = \sum_{i,j} a_{ij}\alpha^i\beta^j, \quad a_{ij} \in K,$$

dove la sommatoria é una somma finita poiché $[L : K] = p^2 < \infty$. Ricordando che siamo in caratteristica p si ha

$$\gamma^p = \left(\sum_{i,j} a_{ij}\alpha^i\beta^j\right)^p = \sum_{i,j} a_{ij}^p\alpha^{ip}\beta^{jp},$$

e pioché $\alpha^p = u$ e $\beta^p = t$ si ottiene

$$\gamma^p = \sum_{i,j} a_{ij}^p u^i t^j.$$

Quindi $\gamma^p \in K$ perché combinazione di elementi di K, ma allora γ é radice del polinomio $x^p - \gamma^p \in K[x]$. Cosí il polinomio minimo di γ su K avrá grado minore di p e di conseguenza $[K(\gamma) : K] \leq p < p^2$. Vista l'arbitrarietá della scelta di γ e tenendo conto del fatto che $[L : K] = p^2$, risulta che $L \neq K(\gamma)$ per ogni $\gamma \in L$. Abbiamo cosí dimostrato che L/K non ha elemento primitivo.

Il Corollario 3.5 ci dice che *tutte le estensioni di campi finite e separabili hanno elemento primitivo (in genere non unico)*. Ma abbiamo visto nell'esempio 2.12 come l'estensione finita $K \subset L = K(\alpha)$ non sia separabile ma abbia lo stesso un elemento primitivo α.
Esiste dunque un criterio che ci permetta di stabilire a priori se un'estensione finita é semplice oppure no? Il seguente teorema dovuto a Steinitz caratterizza tutte le estensioni finite che ammettono elemento primitivo:

Teorema 3.7. *Sia F una estensione finita di K. Allora F é una estensione semplice di K (i.e. F/K ammette elemento primitivo) se e solo se l'estensione F/K ha un numero finito di sottocampi intermedi.*

Dimostrazione. Se K é un campo finito, anche l'estensione finita F lo é. Dunque F é un'estensione semplice di K (l'abbiamo gia dimostrato). Ogni campo intermedio sará un K-sottospazio vettoriale del K-spazio vettoriale F, il quale ha dimensione su K finita, quindi ci sará un numero finito di campi intermedi.
Supponiamo dunque che K sia infinito. Poiché F/K é finita, il Teorema 1.17 mi dice che $F = K(\alpha_1, \ldots, \alpha_n)$, $n \geq 1$. Supponiamo che F/K abbia un numero finito di campi intermedi e mostriamo che é un'estensione semplice. Poiché anche l'estensione $K \subseteq K(\alpha_1, \ldots, \alpha_{n-1})$ avrá un numero finito di campi intermedi, per induzione su n, basta considerare il caso di due elementi algebrici, cioé $F = K(\alpha, \beta)$.
Poiché i campi del tipo $K(\alpha + c\beta)$ sono, al variare di $c \in K$, in numero finito, esistono $c_1, c_2 \in K$ tali che $K(\alpha + c_1\beta) = K(\alpha + c_2\beta) =: L$. Chiaramente vale $L \subseteq K(\alpha, \beta)$. D'altra parte, poiché $\alpha + c_1\beta$, $\alpha + c_2\beta$, c_1, $c_2 \in L$, allora

$$\beta = \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} \quad \in L$$

perché scritto come combinazione di elementi di L ed anche

$$\alpha = (\alpha + c_1\beta) - c_1\beta \quad \in L$$

per lo stesso motivo. Perció $K(\alpha, \beta) \subseteq L$ perché L contiene K, α, β e quindi contiene il piú piccolo campo che li contiene. Dalle due inclusioni si ottiene che $F = K(\alpha, \beta) = L$, cioé l'estensione é semplice.
Viceversa, mostriamo che ogni estensione algebrica semplice $F := K(\alpha)$ ha un numero finito di campi intermedi. Sia $p(x)$ il polinomio minimo di α su K. Se L é un campo intermedio, certamente il polinomio minimo $p_L(x)$ di α su L divide $p(x)$ in $L[x]$ (questo perché polinomio minimo dello stesso elemento in un campo piú grande, dove cioé alcuni fattori irriducibili possono sparire), e se questo é vero in $L[x]$, a maggior ragione $p_L(x) \mid p(x)$ in $F[x]$. Ma questi

possibili $p_L(x)$ sono in numero finito, infatti sicuramente F é contenuto in un campo di spezzamento di $p(x)$ e, per definizione di campo di spezzamento, su tale campo $p(x)$ spezza in fattori lineari

$$p(x) = (x - \gamma_1)(x - \gamma_2) \cdot \ldots \cdot (x - \gamma_d)$$

dove d é il grado di $p(x)$ e gli γ_i non sono necessariamente distinti. Quindi in $F[x]$ il polinomio $p(x)$ ha al massimo

$$\binom{d}{1} + \binom{d}{2} + \ldots + \binom{d}{d} = 2^d - 1$$

divisori monici, che quindi sono in numero finito.
Definiamo quindi una corrispondenza tra i sottocampi intermedi di $K \subseteq F$ e i polinomi minimi di α su tale sottocampo, cioé:

$$\{K \subseteq L \subseteq F\} \longrightarrow \{p_L(x)\}$$

Basta quindi far vedere che tale corrispondenza é iniettiva, e dalla finitezza di $\{p_L(x)\}$ si deduce quello che vogliamo dimostrare.
Sia L' il sottocampo di L generato su K dai coefficienti di $p_L(x)$. Si ha la seguente catena di estensioni $K \subseteq L' \subseteq L \subseteq F$. Poiché $p_L(x) \in L'[x] \subseteq L[x]$ e $p_L(x)$ é irriducibile su L, a maggior ragione $p_L(x)$ é irriducibile anche su L'. Dunque $p_L(x)$ é anche il polinomio minimo di α su L', cioé $p_L(x) = p_{L'}(x)$. Ne segue che $L(\alpha) = L'(\alpha)$, e valgono

$$[L'(\alpha) : L'] = [L(\alpha) : L], \tag{3.6}$$

e

$$[L(\alpha) : L'] = [L'(\alpha) : L']. \tag{3.7}$$

Si ha $L' \subseteq L \subseteq L(\alpha)$ e applicando il Teorema 1.12 e i risultati 3.6 e 3.7 ottenuti si trova

$$[L(\alpha) : L'] = [L(\alpha) : L] \cdot [L : L']$$

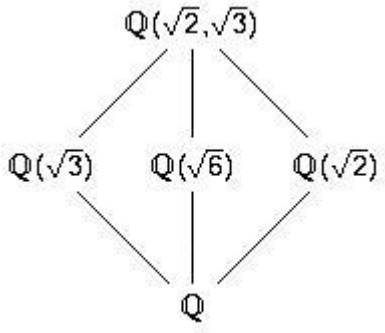
$$[L'(\alpha) : L'] = [L(\alpha) : L] \cdot [L : L']$$

$$1 = [L : L']$$

da cui segue che $L = L'$. In conclusione il campo intermedio L é univocamente determinato dai coefficienti di $p_L(x)$, e perció l'applicazione che associa ad L il polinomio $p_L(x)$ é iniettiva, da cui l'asserto.

□

Esempio 3.8. Abbiamo visto nell'esempio 3.2 come l'estensione $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sia semplice, e che possiamo prendere $\sqrt{2} + \sqrt{3}$ come elemento primitivo. Il Teorema 3.7 mi dice quindi che esiste un numero finito di campi intermedi tra $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ $(= \mathbb{Q}(\sqrt{2}+\sqrt{3}))$. L'intera struttura di inclusioni di campi é mostrata nel diagramma sottostante:



Infatti $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ e come é fatta una sua base su $\mathbb{Q}$? Potendo ottenere $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ mediante due estensioni di grado 2, un elemento di $\mathbb{Q}(\sqrt{2})$ si scrive come

$$a + b\sqrt{2} \quad \text{con} \quad a, b \in \mathbb{Q}$$

ed un elemento di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ si scrive come

$$\alpha + \beta\sqrt{3} \quad \text{con} \quad \alpha, \beta \in \mathbb{Q}(\sqrt{2})$$

quindi

$$\begin{aligned} \alpha + \beta\sqrt{3} = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = \\ = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \quad \text{con} \quad a, b, c, d \in \mathbb{Q} \end{aligned}$$

perció $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é una base di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ su $\mathbb{Q}$. Inoltre essendo $4 = 2 \cdot 2$, ogni campo intermedio deve avere grado 2 su $\mathbb{Q}$, quindi posso

generarlo prendendo per basi $\{1, \sqrt{2}\}$, $\{1, \sqrt{3}\}$, $\{1, \sqrt{6}\}$ e queste sono le sole ammissibili.

Esempio 3.9. Riprendiamo l'esempio 3.6. Avevamo visto che l'estensione

$$K = \mathbb{F}_p(u, t) \subset L$$

non é semplice. In base al Teorema 3.7 esistono quindi infiniti campi intermedi per l'estensione L/K. Vediamo di dimostrarlo.
Consideriamo di nuovo $\alpha, \beta \in L$ con $\alpha^p = u$, $\beta^p = t$ e $L = K(\alpha, \beta)$. Studiamo le estensioni intermedie del tipo

$$K(\alpha + \lambda\beta) \subset L$$

con $\lambda \in K$. Supponiamo che esistano $\lambda \neq \mu \in K$ tali che $K(\alpha + \lambda\beta) = K(\alpha + \mu\beta)$. In questo caso si avrebbe che $\alpha + \mu\beta \in K(\alpha + \lambda\beta)$ e quindi avremmo che:

$$\frac{\alpha + \mu\beta - (\alpha + \lambda\beta)}{\mu - \lambda} = \frac{\beta(\mu - \lambda)}{\mu - \lambda} = \beta \quad \Rightarrow \quad \beta \in K(\alpha + \lambda\beta),$$

da cui

$$\alpha + \lambda\beta - (\lambda\beta) = \alpha \quad \Rightarrow \quad \alpha \in K(\alpha + \lambda\beta).$$

Si ha quindi che $K(\alpha, \beta) \subseteq K(\alpha + \lambda\beta)$. Poiché banalmente vale l'inclusione opposta, si otterrebbe che $K(\alpha, \beta) = K(\alpha + \lambda\beta)$. Questo vorrebbe dire che l'estensione L/K é semplice, in disaccordo con quanto abbiamo giá dimostrato. Quindi facendo variare λ in K ottengo sempre campi $K(\alpha + \lambda\beta)$ distinti. Ma poiché K é infinito, esistono quindi infiniti campi intermedi tra K ed L.

Bibliografia

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

[2] Cox David A., *Galois Theory*. Pure and Applied Mathematics (New York). Wiley-Interscience [John Wiley Sons], Hoboken, NJ, 2004.

[3] Conte A., Picco Botta L., Romagnoli D., *Algebra*, Levrotto&Bella, Torino, Italia, 1986.

[4] Milne J. S., *Fields and Galois Theory*, Version 4.30, april 15, 2012. online su `www.jmilne.org/math/CourseNotes/FT.pdf`

[5] Conrad K., *Separability*, online su `www.math.uconn.edu/kconrad/articles/`