

Per risolvere un'equazione algebrica, il suo polinomio associato deve fattorizzarsi completamente in un'opportuna estensione (CRC).

Def. (Estensione Normale):

Dato $F \subseteq K$ estensione, si dice che K è **ESTENSIONE NORMALE** se:

- 1) K è estensione algebrica
- 2) $\forall b \in K$ il polinomio minimo di b su F si fattorizza completamente in $K[x]$

Si dirà K normale su F .

Esempi:

1) Se $[K:F] = 2$, allora K normale su F :

$\Rightarrow b \in F \vee b \in K \setminus F$ si ha:

$\deg_F b = 2 \Rightarrow$ il polinomio minimo è $x^2 + px + q$ e si fattorizza in $(x-b)(x+b+p)$. Una radice è b , l'altra è $-p-b \in K$

Notiamo che se $b \in K \setminus F$, si ha $K = F(b)$

2) Dato p primo, $\mathbb{Q}(\sqrt[p]{p})$ è normale su $\mathbb{Q}(\sqrt[p]{p})$ (l'estensione ha $\deg = 2$). Analogamente $\mathbb{Q}(\sqrt[4]{p})$ è normale su \mathbb{Q} . Tuttavia $\mathbb{Q}(\sqrt[4]{p})$ non è normale su \mathbb{Q} : il polinomio minimo di $\sqrt[4]{p}$ su \mathbb{Q} è $x^4 - p$ che ha radici non reali

3) Data la catena di estensioni $F \subseteq L \subseteq K$, si ha

che se L è normale su F , allora lo è anche su K .

Teorema:

Sia K estensione finita di F , allora:

$$K \text{ normale su } F \Leftrightarrow \begin{cases} K \text{ è CRC di un certo} \\ \text{polinomio } f(x) \in F[x] \end{cases}$$

Dim.:

(\Rightarrow): K normale su $F \Rightarrow [K:F] = m \Rightarrow \{b_1, \dots, b_m\}$ base di K su $F \Rightarrow$ sia $f_i(x)$ polinomio minimo di $b_i \Rightarrow f(x) = f_1(x) \cdots f_m(x) \Rightarrow$ ogni $f_i(x)$ si fattorizza completamente in $K[x] \Rightarrow \exists c_1, \dots, c_n$ radici di $f(x)$ in K . Tra queste ci sono $b_1, \dots, b_m \Rightarrow K = F(b_1, \dots, b_m) \subseteq F(c_1, \dots, c_n) \subseteq K \Rightarrow K = F(c_1, \dots, c_n)$ è il CRC di $f(x)$

(\Leftarrow): K è CRC di $f(x) \in F[x] \Rightarrow$ sia $b \in K$, $g(x)$ il suo polinomio minimo su $F[x]$. Mostriamo che g si fattorizza completamente in $K[x]$:
sia L estensione di K t.c. L è il CRC di g su $F[x] \Rightarrow$ sia c radice di g in L , sicuramente K è il CRC di $f(x)$ su F , quindi è anche il CRC di $f(x)$ su $F(b)$. Ma $K(c)$ è il CRC di $f(x)$ su $F(c) \Rightarrow \exists$ isomorfismo di campi $\varphi: F(b) \rightarrow F(c)$ t.c. $\varphi = \text{Id}_F \Rightarrow$ per l'unicità

del CRC $\exists \eta : K \rightarrow K(c)$ isomorfismo che estende φ . Allora η è in particolare un isomorfismo di spazi vettoriali su $F \Rightarrow [K:F] = [K(c):F]$
 $\Rightarrow [K(c):F] = [K(c):k] \cdot [K:k] \Leftrightarrow [K(c):k] = 1$
 $\Leftrightarrow K(c) = K \Rightarrow c \in K$

q.e.d.

Proposizione:

Se K è normale su F e $b, c \in K$ hanno lo stesso polinomio minimo, allora $\exists F$ -automorfismo $\varphi : K \rightarrow K$ t.c. $\varphi(b) = c$

Estensioni Separabili:

$f(x) \in F[x]$ non ha radici multiple in alcuna estensione di F se e solo se $\text{MCD}\{f, f'\} = 1$

Def. (Polinomio Separabile)

Un polinomio irriducibile $f(x) \in F[x]$ si dice **SEPARABILE** se $\text{MCD}\{f, f'\} = 1$ ovvero se $f'(x) \neq 0$. Se f non è irriducibile, si dice che f è separabile se ogni sua fattore irriducibile è separabile

Proposizione

Se $\text{car } F = 0$, $\forall f(x) \in F[x]$ si ha f separabile

N.B.

I polinomi costanti sono considerati separabili

Def. (Campo Perfetto):

Un campo F si dice **PERFETTO** se ogni polinomio su $F[x]$ è separabile.

\Rightarrow se $\text{car } F = p > 0$ (p primo) possiamo definire l'automorfismo di campi di Frobenius $\varphi: F \rightarrow F$ t.c.
 $\varphi(a) = a^p$ (se $\text{car } F = p$, vale il sogno della matricola)

Teorema:

Se $\text{car } F = p > 0$ (p primo), allora si ha:

$$F \text{ perfetto} \Leftrightarrow F^p = F \text{ con } F^p = \text{Im } (\varphi)$$

(φ automorfismo di campi di Frobenius)

Dim.:

\Rightarrow : F perfetto $\Rightarrow a \in F \Rightarrow f(x) = x^p - a$ è separabile
 \Rightarrow sia $g(x) \in F[x]$ un fattore irriducibile di $f(x)$
 \Rightarrow sia K un CRC di $g(x)$ su F e sia $b \in K$ radice di $g(x)$
 $\Rightarrow f(b) = 0 \Rightarrow b^p - a = 0 \Rightarrow a = b^p$
 $\Rightarrow f(x) = x^p - a = x^p - b^p = (x - b)^p \in K[x]$
 \Rightarrow per l'unicità della fattorizzazione,
 $g(x) = (x - b)^m \in K[x] \Rightarrow$ dato che g è separabile
in $F[x]$, $m=1 \Rightarrow b \in F$
 $\Rightarrow a = b^p \in F^p$

\Leftarrow : $F^p = F \Rightarrow$ sia $f(x) = a_0 + \dots + a_n x^n$ irriducibile
in $F[x]$ e non separabile $\Rightarrow f'(x) = 0$

$$\Rightarrow \alpha_1 + \dots + n \alpha_m x^{m-1} = 0 \Rightarrow i \cdot \alpha_i = 0 \quad \forall i = 1, \dots, m$$

$$\Rightarrow \text{se } p \nmid i, \alpha_i = 0 \Rightarrow f(x) = \alpha_0 + \alpha_p x^p + \dots + \alpha_{mp} x^{mp}$$

$$\Rightarrow \text{per } i = 1, \dots, m, \alpha_{ip} = b_i^p \Rightarrow \text{si ha:}$$

$$f(x) = b_0^p + b_1^p x^p + \dots + b_m^p x^{mp} = (b_0 + b_1 x + \dots + b_m x^m)^p$$

$$\Rightarrow f \text{ riducibile} \quad \Leftrightarrow$$

q.e.d.

\Rightarrow come conseguenza, si ha che ogni campo finito è perfetto.

Controesempio:

$F = \mathbb{F}_p(t)$ (campo delle frazioni di $\mathbb{F}_p[t]$)

$\Rightarrow f(x) = x^p - t \Rightarrow f(x)$ è irriducibile per il Lemma di Gauss e per Eisenstein

Corrispondenza di Galois:

Se K è estensione di F , denotiamo con $\text{Aut}_F(K)$ il gruppo degli F -automorfismi di K . Se F è il sottocampo minimo di K , $\text{Aut}_F(K)$ è il gruppo di tutti gli automorfismi di K . Data la catena di estensioni $F \subseteq E \subseteq K$, si ha $\text{Aut}_E(K)$ è sottogruppo di $\text{Aut}_F(K)$

Def. ($\text{Fix}_K(G)$):

Se G è un sottogruppo di $\text{Aut}_F(K)$, si definisce:

$$\text{Fix}_K(G) = \{\alpha \in K \mid \gamma(\alpha) = \alpha \quad \forall \gamma \in G\}$$

Si ha che $\text{Fix}_K(G)$ è un sottocampo di K contenente F

\Rightarrow Data K estensione di F , $G \leqslant \text{Aut}_F(K)$, si ha che $\text{Fix}_K(G)$ è sottogruppo di K contenente F .

\Rightarrow se E è sottocampo di K contenente F , $\text{Aut}_E(K)$ è sottogruppo di $\text{Aut}_F(K)$

\Rightarrow siano $F \subseteq E \subseteq K$: allora $\text{Fix}_K(\text{Aut}_E(K)) \supseteq E$
 $\Rightarrow G \leqslant \text{Aut}_F(K) \Rightarrow E = \text{Fix}_K(G) \wedge G \leqslant \text{Aut}_E(K)$

\Rightarrow se $G_1 \leqslant G_2 \leqslant \text{Aut}_F(K)$, allora $\text{Fix}_K(G_2) \subseteq \text{Fix}_K(G_1)$

\Rightarrow se $F \subseteq E_1 \subseteq K$, allora $\text{Aut}_{E_2}(K) \leqslant \text{Aut}_{E_1}(K)$

Teorema (Fundamentale della Teoria di Galois):

K è normale e separabile su K se e solo se:

1) $F \subseteq E \subseteq K \Rightarrow \text{Fix}_K(\text{Aut}_E(K)) = E \quad \forall E$ sottocampo

2) $G \leqslant \text{Aut}_F(K) \Rightarrow G = \text{Aut}_{\text{Fix}_K(G)}(K) \quad \forall G$ sottogruppo.

$\Rightarrow K$ si dice ESTENSIONE DI GALOIS

Dati A insieme, K campo, K^A (funzioni di A in K) è spazio vettoriale su K :

$f, g \in K^A \Rightarrow f+g$ t.c. $f+g(a) = f(a) + g(a) \quad \forall a \in A$

$b \in K, f \in K^A \Rightarrow (bf)(a) = b f(a) \quad \forall a \in A$

Proposizione:

Se F è un campo, allora l'insieme degli automorfismi $F \rightarrow K$ è lin. ind. in K^F (ovvero ogni suo sottinsieme finito è lin. ind.)

Dim.:

Sia per assurdo $\{\varphi_0, \dots, \varphi_n\}$ un sottospazio lin. disp. con il minimo numero di elementi $n+1$:

$$\varphi_0 = \sum_{i=1}^n \alpha_i \varphi_i, \quad \alpha_1 \neq 0$$

\Rightarrow siano $b, c \in F$:

$$\sum_{i=1}^n \alpha_i \varphi_i(b) \varphi_i(c) = \sum_{i=1}^n \alpha_i \varphi_i(bc) = \varphi_0(bc) = \varphi_0(b)\varphi_0(c)$$

$$= \varphi_0(b) \sum_{i=1}^n \alpha_i \varphi_i(c) = \sum_{i=1}^n \alpha_i \varphi_i(c) \varphi_0(b)$$

$$\begin{aligned} \Rightarrow 0 &= \sum_{i=1}^n \alpha_i \varphi_i(b) \varphi_i(c) - \sum_{i=1}^n \alpha_i \varphi_i(c) \varphi_0(b) \\ &= \sum_{i=1}^n \alpha_i \varphi_i(b) \varphi_i(c) - \alpha_i \varphi_i(c) \varphi_0(b) \\ &= \sum_{i=1}^n \alpha_i (\varphi_i(b) - \varphi_0(b)) \varphi_i(c) \end{aligned}$$

$$\Rightarrow \sum_{i=1}^n \alpha_i (\varphi_i(b) - \varphi_0(b)) \varphi_i = 0$$

Per costruzione, $\{\varphi_1, \dots, \varphi_n\}$ è lin. ind. !!!

$$\Rightarrow \alpha_i (\varphi_i(b) - \varphi_0(b)) = 0 \quad \forall i = 1, \dots, n$$

$$\Rightarrow \varphi_1(b) - \varphi_0(b) = 0 \quad \forall b \in F \Rightarrow \varphi_1 = \varphi_0 \quad \leftarrow$$

q.e.d.

Lemma (di Dedekind):

Dati F, K campi, $\varphi_i : F \rightarrow K$ ($i = 1, \dots, n$) numeri distinti, sia $L := \{b \in F \mid \varphi_1(b) = \dots = \varphi_n(b)\}$. Allora L è sottocampo di F e $[F : L] \geq n$

Dim.:

Supponiamo $[F : L] = r < n$, sia $\{b_1, \dots, b_r\}$ base di

F su L . Consideriamo la matrice:

$$A = \begin{pmatrix} \varphi_1(b_1) & \dots & \varphi_n(b_1) \\ \vdots & & \vdots \\ \varphi_1(b_m) & \dots & \varphi_n(b_m) \end{pmatrix}$$

$\Rightarrow f: K^m \rightarrow K^n$ con $f(v) = Av$ è lineare e non iniettiva (Teorema Nullità + Range)

$\Rightarrow v = (\alpha_1, \dots, \alpha_m)^T \neq \vec{0}$ t.c. $Av = 0$, allora:

$$\sum_{i=1}^m \alpha_i \varphi_i(b_s) = 0 \quad \forall s = 1, \dots, n$$

\Rightarrow se $b \in F$ si ha:

$$b = c_1 b_1 + \dots + c_n b_n, \quad c_s \in L$$

$$\begin{aligned} \Rightarrow \sum_{i=1}^m \alpha_i \varphi_i(b) &= \sum_{i=1}^m \alpha_i \varphi_i\left(\sum_{s=1}^n c_s b_s\right) = \sum_{i=1}^m \sum_{s=1}^n \alpha_i \varphi_i(c_s b_s) \\ &= \sum_{i=1}^m \sum_{s=1}^n \alpha_i \varphi_i(c_s) \varphi_i(b_s) = \sum_{i=1}^m \sum_{s=1}^n \alpha_i \varphi_i(c_s) \varphi_i(b_s) \end{aligned}$$

$$= \sum_{s=1}^n \varphi_1(b_s) \underbrace{\left[\sum_{i=1}^m \alpha_i \varphi_i(b_s) \right]}_{=0} = 0$$

$\Rightarrow \sum_{i=1}^m \alpha_i \varphi_i(b) = 0 \quad \forall b \in F \Rightarrow \sum_{i=1}^m \alpha_i \varphi_i = 0$ in K^F
tuttavia $\{\varphi_1, \dots, \varphi_n\}$ è lin. ind. $\Leftrightarrow (\alpha_i \neq 0)$

q.e.d.

Caso particolare:

Se $\{\varphi_1, \dots, \varphi_n\}$ è sottogruppo finito di $\text{Aut}_F(K)$, poniamo WLOG $\varphi_1 = \text{Id}$ e ottieniamo:

$$L = \{b \in K \mid \varphi_1(b) = b = \varphi_2(b) = \dots = \varphi_n(b)\} = \text{Fix}_K(G)$$

Def. (Traccia rispetto a G di b)

Sia G sottogruppo di $\text{Aut}_F(K)$, $b \in K$. Si definisce la **TRACCIA RISPETTO A G di b** come:

$$\text{Tr}_G(b) = \sum_{\varphi \in G} \varphi(b)$$

Proprietà di Tr_G :

1) Se $a \in F$, $\text{Tr}_G(a) = |G|a$

2) $\forall b \in K$, $\text{Tr}_G(b) \in \text{Fix}_K(G)$. Infatti:

sia $\varphi \in G$ t.c. $\varphi(\text{Tr}_G(b)) = \sum_{\psi \in G} \varphi \circ \psi(b)$

$\Rightarrow \varphi \mapsto \varphi \circ \psi$ è biiettiva

3) $\text{Tr}_G()$ è F -lineare e non nulla (G è lin. ind.)

Lemma:

$$\text{Im}(\text{Tr}_G) = \text{Fix}_K(G)$$

Dim.:

\subseteq : viste sopra

\supseteq : $b \in \text{Fix}_K(G) \Rightarrow \exists c \in K$ t.c. $\text{Tr}_G(c) \neq 0$

$$\Rightarrow \text{sia } c' = b(\text{Tr}_G(c))^{-1} \in \text{Fix}_K(G)$$

$$\Rightarrow b = c' \text{Tr}_G(c) = c' \sum_{\psi \in G} \psi(c) = \sum_{\psi \in G} c' \psi(c)$$

$$= \sum_{\psi \in G} \psi(c') \psi(c) = \sum_{\psi \in G} \psi(c'c) = \text{Tr}_G(c'c)$$

$$\in \text{Im}(\text{Tr}_G)$$

q.e.d.