

Sia $F \subseteq K$ estensione completa. Consideriamo $\text{Gal}(K/F)$ (automorfismi di K che fissano F). Si ha:

- 1) Se G è sottogruppo di $\text{Gal}(K/F)$, $\text{Fix}_K(G)$ è sottocampo di K contenente F .
- 2) Se E è sottocampo di K contenente F , allora $\text{Gal}(K/E)$ è sottogruppo di $\text{Gal}(K/F)$

Teorema:

Dato $F \subseteq K$, le seguenti sono equivalenti:

- 1) $\exists G$ sottogruppo finito di $\text{Gal}(K/F)$ t.c. $F = \text{Fix}_K(G)$
- 2) K è estensione finita di F e $\text{Fix}_K(\text{Gal}(K/F))$
- 3) K è estensione finita di F e $|\text{Gal}(K/F)| = [K:F]$

Dim.:

$$1) \Rightarrow 2): \checkmark$$

$$2) \Rightarrow 3): \text{Gal}(K/F) \text{ è finito e } [K:F] = |\text{Gal}(K/F)|$$

$$3) \Rightarrow 1): G = \text{Gal}(K/F), E = \text{Fix}_K(G). \text{ Per Artin,}$$

$$[K:E] = |G| \Rightarrow \frac{[K:F]}{|G|} = \frac{[K:E]}{|G|} \cdot \frac{[E:F]}{|G|}$$

$$\Rightarrow [E:F] = 1 \Rightarrow E = F$$

Def. (Estensione di Galois):

Dato $F \subseteq K$, K si dice ESTENSIONE DI GALOIS DI F se soddisfa le ipotesi del teorema sopra (K è estensione finita e $[K:F] = |\text{Gal}(K/F)|$)

Esempi:

- 1) dato $d \in \mathbb{Z}$, $\mathbb{Q}(\sqrt{d})$ è Galois su \mathbb{Q}
- 2) $\mathbb{Q}(\sqrt[3]{2})$ non è Galois su \mathbb{Q}
- 3) dato K campo finito con $\text{car}(K) = p$, K è Galois su \mathbb{F}_p :

1) K è estensione finita

2) $\varphi: K \rightarrow K$ t.c. $\varphi(b) = b^p$ (omorfismo di Frobenius), si ha $\varphi \in \text{Gal}(K/\mathbb{F}_p)$. Inoltre:

$\langle \varphi \rangle$ è sottogruppo finito di $\text{Gal}(K/\mathbb{F}_p)$

$\Rightarrow a \in K \Rightarrow a \in \mathbb{F}_p \Leftrightarrow a^p = a \Rightarrow x - x^p$ ha radici distinte $\Rightarrow \mathbb{F}_p = \text{Fix}_K(\langle \varphi \rangle)$

$\Rightarrow \text{Gal}(K/\mathbb{F}_p) = \langle \varphi \rangle$

Proposizione:

Ogni gruppo di Galois è ciclico

Possiamo ora dimostrare il seguente:

Teorema (Fundamentale della Teoria di Galois):

Sia K estensione di Galois di F , consideriamo l'insieme $\mathcal{E} := \{E \mid F \subseteq E \subseteq K\}$ (insieme dei campi intermedi).

Sia inoltre $\mathcal{L} :=$ insieme dei sottogruppi di $\text{Gal}(K/F)$

Allora $\text{Gal}: \begin{cases} \mathcal{E} & \longrightarrow \mathcal{L} \\ E & \longmapsto \text{Gal}(K/E) \end{cases}$, $\text{Fix}_K: \begin{cases} \mathcal{L} & \longrightarrow \mathcal{E} \\ H & \longmapsto \text{Fix}_K(H) \end{cases}$ sono

2 bijezioni una l'inversa dell'altra. Inoltre si ha che $\forall E \in \mathcal{E}$ K è estensione di Galois di E e vale la seguente: $[E:F] = [\text{Gal}(K/F):\text{Gal}(K/E)]$. Si ha

inoltre che, dato $E \in \mathcal{E}$, le seguenti condizioni sono equivalenti:

- 1) E è Galois su F
- 2) $\text{Gal}(K/E)$ è normale in $\text{Gal}(K/F)$
- 3) $\varphi^*(E) \subseteq E \quad \forall \varphi \in \text{Gal}(K/F)$

Dim.:

1) Mostriamo che $E = \text{Fix}_K(\text{Gal}(K/E))$ con $E \in \mathcal{E}$:

Sia $H = \text{Gal}(K/F)$, $E' = \text{Fix}_K(\text{Gal}(K/E)) \Rightarrow E \subseteq E'$
 $\Rightarrow [E':F] = [E':E] \cdot [E:F]$, quindi ci basta mostrare che $[E':F] \leq [E:F]$. Dato che $E' = \text{Fix}_K(\cdot)$, si ha che K è certamente Galois su E' e $H = \text{Gal}(K/E')$.

$$\text{Sia } r = [E':F] = \frac{[K:F]}{[K:E']} = \frac{|\text{Gal}(K/F)|}{|\text{Gal}(K/E')|} = [\text{Gal}(K/F):H]$$

Siano $t_1 H, \dots, t_r H$ le classi laterali sinistre.

$$\begin{aligned} &\text{Se } \alpha, \beta \in \text{Gal}(K/F), \alpha H = \beta H \Leftrightarrow \alpha^{-1}\beta \in H \\ &\Leftrightarrow \alpha^{-1}\beta(b) = b \quad \forall b \in E \Leftrightarrow \alpha(b) = \beta(b) \quad \forall b \in E \end{aligned}$$

Quindi t_1, \dots, t_r inducono (mediante restrizione ad E) $\varphi_1, \dots, \varphi_r : E \rightarrow K$ monomorfismi distinti

Assumiamo WLOG $t_1 = \text{Id}$, allora t_1 è inclusione $E \rightarrow K$. Sia $F' = \{b \in E \mid b = \varphi_1(b) = \dots = \varphi_r(b)\} \subseteq E$.

Mostriamo che $F' = F$:

occorre vedere che $F' = \text{Fix}_K(\text{Gal}(K/F))$.

Se $\tau \in \text{Gal}(K/F)$, $\tau = t_i \tau$ per un certo i , per un certo $\tau \in H$. Se $a \in F'$, $\tau(a) = t_i \tau(a) = t_i(a)$

$\varphi(\tau(a)) = a$. Per Dedekind, $r \leq [E : F']$ e
 $r = [E' : F]$

$$\Rightarrow E = \text{Fix}_K(\text{Gal}(K/F))$$

\Rightarrow La corrispondenza di Galois tra E e L è perfetta

2) Mostriamo le 3 condizioni equivalenti:

Sia $\varphi \in \text{Gal}(K/F) \Rightarrow K$ è Galois su $\varphi^*(E)$

$\Rightarrow \text{Gal}(K/\varphi^*(E))$ sono gli automorfismi $\tau \in \text{Gal}(K/F)$

$$\text{l.c. } \tau\varphi(b) = \varphi(b) \quad \forall b \in E \Rightarrow b = \varphi^{-1}\tau\varphi(b)$$

$\Rightarrow \text{Gal}(K/\varphi^*(E)) = \varphi^{-1}H\varphi$ con $H = \text{Gal}(K/E)$

Altro:

$$[K:\varphi^*(E)] = |\text{Gal}(K/\varphi^*(E))| = |\varphi^{-1}H\varphi| = |H| = [K:E]$$

Se vale 2) abbiamo $\varphi^{-1}H\varphi = H$ quindi:

$$\varphi^*(E) = \text{Fix}_K(\varphi^{-1}H\varphi) = \text{Fix}_K(H) = E$$

quindi vale 3)

Supponiamo che valga 3). Dato $\varphi \in \text{Gal}(K/F)$, mostriamo che $\varphi^{-1}H\varphi = H = \text{Gal}(K/E)$ ovvero che $\text{Fix}_K(\varphi^{-1}H\varphi) = E$. Sia $\tau \in H, b \in E \Rightarrow \varphi(b) \in E$
 $\Rightarrow \tau(\varphi(b)) = \varphi(b) \Rightarrow \varphi^{-1}(\tau(\varphi(b))) = b$ quindi vale 2). Supponiamo che valga 1), allora $|\text{Gal}(K/F)| = [E:F] = r \Rightarrow \text{Gal}(E/F) = \{\tau_1 = \text{Id}, \tau_2, \dots, \tau_r\}$
Se non vale 3), $\exists \varphi \in \text{Gal}(K/F)$ l.c. $\varphi^*(E) \neq E$. Allora $\varphi|_E = \tau_0 : E \rightarrow K$ è automorfismo distinto da τ_1, \dots, τ_r . Sia $F' = \{a \in E \mid a = \tau_1(a) = \dots = \tau_r(a)\}$,

per Dedekind $[E : F'] \geq r+1$. Data che E è Galois su F , $F = F'$ $\Leftrightarrow 1) \Rightarrow 3) \checkmark$

Supponiamo che valga 3): $\varphi^*(E) \subseteq E \quad \forall \varphi \in \text{Gal}(K/F)$
 $\Rightarrow \varphi^*(E) = E \Rightarrow$ ogni $\varphi \in \text{Gal}(K/F)$ induce un elemento di $\text{Gal}(E/F)$ tramite restrizione. Sia:

$$\nu : \text{Gal}(K/F) \xrightarrow{\varphi} \text{Gal}(E/F)$$

con $\hat{\varphi} : E \rightarrow E$ t.c. $\hat{\varphi}(b) = \varphi(b)$

$\Rightarrow \nu$ è un omomorfismo di gruppi (ovvio), ker ν consiste nei φ che inducono Id su E , quindi è $\text{Gal}(K/E)$.

Per Lagrange e per Artin:

$$|\text{Im } (\nu)| = \frac{|\text{Gal}(K/F)|}{|\text{Gal}(K/E)|} = [E : F] \leq |\text{Gal}(E/F)| \leq [E : F]$$

$\Rightarrow \nu$ è suriettiva \Rightarrow per il teorema di unomorfismi

si ha: $\text{Gal}(E/F) \cong \text{Gal}(K/F)/\text{Gal}(K/E)$

$\Rightarrow |\text{Gal}(E/F)| = [E : F] \Rightarrow E$ è Galois su F

q.e.d.

Applicazioni del Teorema Fondamentale:

Teorema:

Dato K Galois su F , $b \in K$, sia

$$\{\varphi(b) \mid \varphi \in \text{Gal}(K/F)\} = \{b_1, \dots, b_r\} \text{ (distinti)}$$

Allora $f(x) = (x - b_1) \cdots (x - b_r)$ è il polinomio minimo di b su F . In particolare K è estensione finita, normale e separabile di F .

Dim.:

$\varphi \in \text{Gal}(K/F) \Rightarrow \exists \varphi_x : K[x] \rightarrow K[x]$ t.c. $\varphi_x(b) = \varphi(b)$ e $\varphi_x(x) = x$. $P_b = \{b_1, \dots, b_r\} \Rightarrow \varphi$ induce una permutazione di P_b , ma $P_b = \{\varphi(b_1), \dots, \varphi(b_r)\}$. Si ha:

$$\begin{aligned}\varphi_x(f(x)) &= \varphi_x((x - b_1) \cdots (x - b_r)) \\ &\stackrel{|}{=} (x - \varphi(b_1)) \cdots (x - \varphi(b_r)) = f(x)\end{aligned}$$

\Rightarrow i coefficienti di $f(x)$ sono fissati da ogni $\varphi \in \text{Gal}(K/F)$, quindi $f(x) \in F[x]$

Sia h il polinomio minimo di b su F , allora $h \mid f$ (fra le radici di f c'è anche b). $b_i = \varphi(b)$ per un certo $\varphi \in \text{Gal}(K/F)$. Calcoliamo:

$$\begin{aligned}h(b_i) &= h(\varphi(b)) = \alpha_0 + \alpha_1 \varphi(b) + \dots + \alpha_n \varphi(b)^n \\ &= \varphi(\alpha_0) + \varphi(\alpha_1) \varphi(b) + \dots + \varphi(\alpha_n) \varphi(b)^n \\ &= \varphi(\alpha_0 + \alpha_1 b + \dots + \alpha_n b^n) = 0\end{aligned}$$

$\Rightarrow b_1, \dots, b_r$ sono radici di $h \Rightarrow \deg h \geq \deg f = r$
 $\Rightarrow h = f$

q.e.d.

Teorema:

Dato K estensione di F , sono equivalenti le seguenti:

- 1) K è Galois su F
- 2) K è estensione finita, normale e separabile di F
- 3) K è CRC per un polinomio separabile in $F[x]$

Dim.:

1) \Rightarrow 2) ✓

2) \Rightarrow 3) ✓

3) \Rightarrow 1):

Sia K CRC di $f(x) \in F[x]$ separabile.

Sia $F' = \text{Fix}_K(\text{Gal}(K/F))$, mostriamo che $F' = F$
 \Rightarrow l'equazione su m : numero di radici di f in $K \setminus F$
 $m = 0 \Rightarrow K = F$ ✓

$m > 0$:

$$b \in K \setminus F \text{ t.c. } f(b) = 0$$

\Rightarrow sia $E = F(b)$, K è CRC di $f(x)$ su E

\Rightarrow per ipotesi induktiva, K è Galois su E

$\Rightarrow F(b)$ ha base $\{1, b, \dots, b^{m-1}\}$ su F se $h(x)$ polinomio minimo di b su F ha deg = m

\Rightarrow Sia $a \in F' \subseteq E = \text{Fix}_K(\text{Gal}(K/E))$ con
 $\text{Gal}(K/E) \leqslant \text{Gal}(K/F)$, allora:

$$a = c_0 + c_1 b + \dots + c_{m-1} b^{m-1} \text{ con } c_i \in F$$

\Rightarrow dato che K è normale su F e h ha radice in K , $h(x)$ si fattorizza in $K[x]$. Inoltre $h(x) | f(x)$ dato che $f(b) = 0$

$\Rightarrow h$ è separabile \Rightarrow siano $b_1 = b, b_2, \dots, b_m$ le radici distinte di h in K

$\Rightarrow \forall i \exists \varphi_i \in \text{Gal}(K/E) \text{ t.c. } b_i = \varphi_i(b)$

$$\Rightarrow a = \varphi_i(a) = \varphi_i(c_0 + \dots + c_{m-1} b^{m-1})$$

$$= c_0 + c_1 b_i(b) + \dots + c_{n-1} b_i^{n-1}$$

$$= c_0 + c_1 b_i + \dots + c_{n-1} b_i^{n-1}$$

$$\Rightarrow \text{allora } g(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} - a \in E[x]$$

ha n radici distinte e $\deg g \leq n-1$

$$\Rightarrow g(x) = 0 \Rightarrow c_0 = a, c_1 = \dots = c_{n-1} = 0$$

$$\Rightarrow a = c_0 \in F \checkmark$$

q.e.d.

Esempio:

Dati p, q primi distinti, si ha:

$$K = \mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

Infatti:

$$\subseteq : \checkmark$$

$$\supseteq : \frac{1}{\sqrt{p} + \sqrt{q}} = \frac{\sqrt{p} - \sqrt{q}}{p - q} \Rightarrow \sqrt{p} - \sqrt{q} \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$$

$$\text{quindi } 2\sqrt{p}, 2\sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q}) \checkmark$$

Si ha inoltre che $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$:

$$a + b\sqrt{p} = \sqrt{q} \Rightarrow a^2 + 2ab\sqrt{p} = q$$

$$\Rightarrow 2ab\sqrt{p} = q - b^2p - a^2 \Rightarrow ab = 0 \wedge q - b^2 - a^2 = 0$$

$$\Rightarrow a = 0 \Rightarrow b^2 = \frac{q}{p} \quad \checkmark$$

$$\Rightarrow b = 0 \Rightarrow a^2 = q \quad \checkmark$$

$$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$$

$$\Rightarrow [K : \mathbb{Q}] = 4 \Rightarrow b = \sqrt{p} + \sqrt{q} \Rightarrow \sqrt{q} = b - \sqrt{p}$$

$$\Rightarrow q = b^2 - 2b\sqrt{p} + p \Rightarrow 2b\sqrt{p} = b^2 + p - q$$

$$\Rightarrow 4b^2p = b^4 + p^2 + q^2 + 2b^2p - 2b^2q - 2pq$$

$\Rightarrow b$ è radice di $x^4 - 2(p+q)x^2 + (p-q)^2$

\Rightarrow le radici sono $\pm\sqrt{p}, \pm\sqrt{q} \in K$

$\Rightarrow K$ è CRC di $x^4 - 2(p+q)x^2 + (p-q)^2$ e quindi
 K è Galois su \mathbb{Q}

$\Rightarrow |\text{Gal}(K/\mathbb{Q})| = 4$. Troviamo gli automorfismi:

$$\varphi \in \text{Gal}(K/\mathbb{Q}) \Rightarrow \varphi(\sqrt{p})^2 = \varphi(p) = p$$

K ha base $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ su \mathbb{Q} , quindi:

$$\varphi(\sqrt{p}) = \pm\sqrt{p}, \quad \varphi(\sqrt{q}) = \pm\sqrt{q}$$

$$\Rightarrow \text{Id}: \sqrt{p} \mapsto \sqrt{p}, \sqrt{q} \mapsto \sqrt{q}$$

$$\Rightarrow \varphi_1: \sqrt{p} \mapsto \sqrt{p}, \sqrt{q} \mapsto -\sqrt{q}$$

$$\Rightarrow \varphi_2: \sqrt{p} \mapsto -\sqrt{p}, \sqrt{q} \mapsto \sqrt{q}$$

$$\Rightarrow \varphi_3: \sqrt{p} \mapsto -\sqrt{p}, \sqrt{q} \mapsto -\sqrt{q}$$

\Rightarrow si ha:

$\varphi_1^2 = \varphi_2^2 = \varphi_3^2 = \text{Id} \Rightarrow \text{Gal}(K/\mathbb{Q})$ è il
gruppo di Klein!!!

\Rightarrow sottogruppi di $\text{Gal}(K/\mathbb{Q})$:

$$\{\text{Id}\}, \{\text{Id}, \varphi_1\}, \{\text{Id}, \varphi_2\}, \{\text{Id}, \varphi_3\}, \text{Gal}(K/\mathbb{Q})$$

\Rightarrow ci sono quindi 3 campi intermedi.

Se $E_1 = \text{Fix}_K(\{\text{Id}, \varphi_1\})$, $\text{Gal}(K/E_1) = \{\text{Id}, \varphi_1\}$

\Rightarrow polinomio minimo di $b = \sqrt{p} + \sqrt{q}$ su E_1 :

$$(x-b)(x-\varphi_1(b)) = \dots = x^2 - 2\sqrt{p}x + p - q$$

\Rightarrow in particolare, $\sqrt{p} \in E_1 \Rightarrow E_1 = \mathbb{Q}(\sqrt{p})$,

$$E_2 = \text{Fix}_K(\{\text{Id}, \varphi_2\}) = \mathbb{Q}(\sqrt{q})$$

$$E_3 = \text{Fix}_K(\{\text{Id}, \varphi_3\}) = \mathbb{Q}(\sqrt{pq})$$

Def. (Elemento primitivo):

Se K è un'estensione finita di F , un **ELEMENTO PRIMITIVO** è un $b \in K$ t.c. $K = F(b)$

Teorema (dell'elemento primitivo):

Se K è un'estensione finita e separabile di F , allora $\exists b \in K$ primitivo ($K = F(b)$)

Dim.:

Caso difficile: F infinito

$\Rightarrow K = F(b_1, \dots, b_n)$, sia $f_i(x)$ polinomio minimo di b_i su F , si ha:

$$f(x) = f_1(x) \cdots f_n(x) \text{ è separabile}$$

$\Rightarrow K'$ è CRC di f su K ed è Galois su K

$\Rightarrow K'$ è Galois su $F \Rightarrow \exists$ numero finito n di campi intermedi $F \subseteq E \subseteq K$

Se $n=1$ V,

se $n > 1$:

$F(b_1 + \alpha b_2)$ con $\alpha \in F$ sono campi t.c.

$$F \subseteq F(b_1 + \alpha b_2) \subseteq K$$

$\Rightarrow \exists \alpha_1, \alpha_2 \in F$ con $\alpha_1 \neq \alpha_2$ t.c.:

$$F(b_1 + \alpha_1 b_2) = F(b_1 + \alpha_2 b_2)$$

\Rightarrow Ponendo $b_{1,2} = b_1 + \alpha_1 b_2$, $F(b_1, b_2) = F(b_{1,2})$
quindi $K = F(b_1, \dots, b_n) = F(b_{1,2}, b_3, \dots, b_n)$ e
la tesi si ha per induzione.

Caso facile: F finita

$\Rightarrow K$ è finita \Rightarrow se $\text{car } K = p \wedge K = \mathbb{F}_p(b)$, si avrà
 $K = F(b) \Rightarrow K \setminus \{0\}$ è ciclico \Rightarrow se b è un
generatore, $K = \{0\} \cup \{1, b, \dots, b^{p^m-2}\}$ con $|K| = p^m$
 $\Rightarrow K \subseteq \mathbb{F}_p(b) \subseteq K \Rightarrow K = \mathbb{F}_p(b)$

q.e.d.

Apparato dimostrativo sull'equazione cubica:

Consideriamo una generica equazione cubica

$$y^3 + ay^2 + by + c = 0$$

\Rightarrow sostituiamo $y = x - k$, k arbitrario:

$$x^3 - 3kx^2 + 3k^2x + k^3 + ax^2 - 2akx + ak^2 + bx - bk + c = 0$$

\Rightarrow scegliendo $k = \frac{a}{3}$ si ha:

$$x^3 + 3px + 2q = 0, \quad p, q \text{ opportuni}$$

\Rightarrow sostituiamo $x = u + v$:

$$u^3 + \underbrace{3u^2v + 3uv^2 + v^3}_{= 3uv(u+v)} + \underbrace{3pu + 3pv + 2q}_{= 3p(u+v)} = 0$$

$$\Rightarrow u^3 + 3(uv + p)(u+v) + v^3 + 2q = 0$$

\Rightarrow supponiamo $u \neq 0$ e scegliamo $v = -\frac{p}{u}$:

$$u^3 - \frac{p^3}{u^3} + 2q = 0 \Leftrightarrow (u^3)^2 + 2qu^3 - p^3 = 0$$

$$\Leftrightarrow u^3 = -q + \sqrt[p]{p^3 + q^2}, \quad v = -q - \sqrt[p]{p^3 + q^2}$$

\Rightarrow supponendo $p^3 + q^2 > 0$, si ricava la **FORMULA DI CARDANO**:

$$x = \sqrt[3]{-q + \sqrt[p]{p^3 + q^2}} + \sqrt[3]{-q - \sqrt[p]{p^3 + q^2}}$$