CAMPI

giovedì 23 novembre 2023 16:04

ESTENSIONI ED ESTENSIONI ALGEBRICHE

- K, F campi, $K \subseteq F$, F si dice **estensione** di K e si denota con F/K

- F/K, $\alpha \in F$ si dice **algebrico** su K se $\exists\, f(x) \in K[x]$, $f(x) \neq 0$ t.c. $f(\alpha) = 0$

- F/K, $\alpha \in F$ si dice **trascendente** su K se $\nexists\, f(x) \in K[x]$, $f(x) \neq 0$ t.c. $f(\alpha) = 0$
(cioè se non è algebrico)

- F/K, $\alpha \in F$ si dice **algebrico** su K se $\{1, \alpha, \dots, \alpha^n\}$ sono lin. dip.
con $f(\alpha) = a_n\alpha^n + \dots + a_1\alpha + a_0$

- F/K, $\alpha \in F$ si dice **trascendente** su K se $\{1, \alpha, \dots, \alpha^n\}$ sono lin. indip.
cioè $f(\alpha) = a_n\alpha^n + \dots + a_1\alpha + a_0 = 0 \iff a_i = 0 \ \forall i$

- F/K si dice **algebrica** su K se $\forall \alpha \in F$, α è algebrico su K

- F/K, $\alpha \in F$ $\quad \varphi_\alpha : K[x] \longrightarrow F$, $f(x) \longmapsto f(\alpha)$ è **omo di valutazione**

$$\varphi_\alpha(K[x]) = \mathrm{Im}\,\varphi_\alpha = K[\alpha] = \{ f(\alpha) \mid f(x) \in K[x] \} \subseteq F$$

$$\begin{tikzcd}
K[x] \arrow[r, two heads, "\varphi_\alpha"] \arrow[d, two heads] & K[\alpha] \\
\frac{K[x]}{\mathrm{Ker}\,\varphi_\alpha} \arrow[ur, "\sim", "\overline{\varphi}"'] \arrow[ur, phantom, bend left, "\circlearrowleft"] &
\end{tikzcd}$$

$$\mathrm{Ker}\,\varphi_\alpha = \{ f(x) \in K[x] \mid \varphi_\alpha(f(x)) = f(\alpha) = 0 \}$$

$$\frac{K[x]}{\mathrm{Ker}\,\varphi_\alpha} \cong K[\alpha]$$

- F/K, $\alpha \in F$ $\quad \alpha$ è **algebrico** su $K \iff \mathrm{Ker}\,\varphi_\alpha \neq \{0\} \iff \varphi_\alpha$ non è inj

- F/K, $\alpha \in F$ $\quad \alpha$ è **trascendente** su $K \iff \mathrm{Ker}\,\varphi_\alpha = \{0\} \iff \varphi_\alpha$ è inj $\iff K[x] \cong K[\alpha]$

- $K[\alpha]$ è il minimo sottoanello di L contenente K e α
- $K(\alpha)$ è il minimo sottocampo di L contenente K e α $\Big\}\ \alpha \in L$.
  ↳ è un'estensione semplice di K.

POLINOMI MINIMI

- Dato il pol. $\mu_\alpha(x) \in \mathrm{Ker}\,\varphi_\alpha$ monico e di grado minimo tra i pol. di $\mathrm{Ker}\,\varphi_\alpha$ si ha:

1. $\mu_\alpha(x)$ è irrid. in $K[x]$
2. $\mathrm{Ker}\,\varphi_\alpha = (\mu_\alpha(x))$
3. $\mu_\alpha(x)$ è l'unico pol. monico irriducibile nel nucleo dell'omo di valutazione che si annulla in α

F/K, $\alpha \in F$ α algebrico su K def. **pol. minimo** di α su K, l'unico pol
1) monico
2) irriducibile
3) che si annulla in α ($\in \mathrm{Ker}\,\varphi_\alpha$)

$\text{pol. minimo} = \mu_\alpha(x)$

in particolare $\mathrm{Ker}\,\varphi_\alpha = (\mu_\alpha(x))$

- Dato il pol. $\mu_\alpha(x) \in \operatorname{Ker}\varphi_\alpha$ monico e di grado minimo tra i pol. di $\operatorname{Ker}\varphi_\alpha$ si ha:

  1. $\mu_\alpha(x)$ e' irrid. in $K[x]$
  2. $\operatorname{Ker}\varphi_\alpha = (\mu_\alpha(x))$
  3. $\mu_\alpha(x)$ è l'unico pol. monico irriducibile nel nucleo dell'omo di valutazione che si annulla in α

F/K, $\alpha \in F$ algebrico su K def. pol. minimo di α su K, l'unico pol 1) monico 2) irriducibile 3) che si annulla in α ($\in \operatorname{Ker}\varphi_\alpha$)

$\text{pol. minimo} = \mu_\alpha(x)$

in particolare $\operatorname{Ker}\varphi_\alpha = (\mu_\alpha(x))$

$$\begin{tikzcd} K[x] \arrow[r, two heads, "\varphi_\alpha"] \arrow[d, two heads] & K[\alpha] \\ \frac{K[x]}{(\mu_\alpha(x))} \arrow[ur, "\bar\varphi"'] & \end{tikzcd}$$

$$\boxed{\frac{K[x]}{(\mu_\alpha(x))}} \cong K[\alpha]$$

campo $\Longrightarrow$ campo

$K[\alpha]$ è sp. v. su K e

$\dim_K(K[\alpha]) = \deg\mu_\alpha(x)$ con base $\{1, \alpha, \dots, \alpha^{\deg\mu_\alpha(x)-1}\}$

- $K(\alpha) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ g(x) \neq 0 \right\} \stackrel{=}{} K[\alpha]$ — $=$ vera se α è alg. su K

  $K(\alpha)$: insieme delle fraz. razionali a coeff. in K

ESTENSIONI SEMPLICI

- F/K $[F:K] = \dim_K F$ = grado dell'estensione

- $\alpha \in F$ alg. su K si ha $[K(\alpha):K] = \deg\mu_\alpha(x)$

  $K(\alpha)$: estensione semplice

- F/K, $[F:K] < +\infty$ (grado finito) $\Rightarrow$ F e' est. alg. di K
  Il viceversa e' in generale falso

- L/F e F/K $\Rightarrow$ $K \subseteq F \subseteq L$ cioè L/K — $L \mid F \mid K$ si chiama torre di estensioni

- Teorema dei gradi nelle torri di estensione

  $K \subseteq F \subseteq L$ con $[F:K] = n$ e $[L:F] = m$ $\Rightarrow$ $[L:K] = n.m$

  $L \stackrel{m}{\mid} F \stackrel{n}{\mid} K$ — $n.m$

  F/K, $\alpha \in F$ si ha che $[K(\alpha):K] \mid [F:K]$

ESTENSIONI NON SEMPLICI

- F/K, $\alpha_1, \dots, \alpha_n \in F$ alg. in K. $K[\alpha_1, \dots, \alpha_n] = \{ p(\alpha_1, \dots, \alpha_n) \mid p(x) \in K[x_1, \dots, x_n] \}$
  $\hookrightarrow$ estensione non semplice

- $K[\alpha_1, \dots, \alpha_n]$ e' un campo, e' il più piccolo sottocampo di F che contiene K e $\alpha_1, \dots, \alpha_n$

- $[K[\alpha,\beta]:K] = \deg \underset{K[\beta]}{\mu_\alpha(x)} = \deg \underset{K[\alpha]}{\mu_\beta(x)}$

- $K \subseteq F \subseteq L$ $\alpha \in F$ alg. su K $\mu_{\alpha/L}(x) \mid \mu_{\alpha/K}(x)$ perchè $\mu_{\alpha/K}(x) \in (\mu_{\alpha/L}(x))$

CHIUSURA ALGEBRICA

CHIUSURA ALGEBRICA

- Un campo L si dice algebricamente chiuso se ogni pol. non cost di $L[x]$ ammette almeno una radice in L

- Data un'estensione $\overline{K}/K$, $\overline{K}$ si dice chiusura algebrica di K se:

  1) $\overline{K}$ è algebricamente chiuso

  2) $\overline{K}$ e' algebrico su K (tutti gli elt di $\overline{K}$ sono alg. su K)

- Ogni campo ammette una chiusura algebrica e questa è unica a meno di iso sul campo

CAMPI DI SPEZZAMENTO

- K campo e $\overline{K}$ la sua chiusura algebrica, $f(x) \in K[x]$ non cost.
  $\alpha_1, \dots, \alpha_n \in \overline{K}$ le sue radici nella chiusura algebrica,
  si dice campo di spezzamento il campo $K(\alpha_1, \dots, \alpha_n) \subseteq \overline{K}$

  Il campo di spezzamento di $f(x) \in K[x]$ e' il più piccolo sottocampo della sua chiusura algebrica $\overline{K}$ che contiene tutte le radici di $f(x)$.

CARATTERISTICA DI UN CAMPO

- K campo, $\varphi : \mathbb{Z} \longrightarrow K$
  $1 \longmapsto 1_K : n : \longrightarrow \underbrace{(1_K + \dots + 1_K)}_{n\text{-volte}}$

- $\text{char } K = \begin{cases} 0 & \text{se } \operatorname{Ker}\varphi = \{0\} \Rightarrow \mathbb{Z}/_{\operatorname{Ker}\varphi} = \mathbb{Z} \\ p & \text{se } \operatorname{Ker}\varphi = p\mathbb{Z} \Rightarrow \mathbb{Z}/_{\operatorname{Ker}\varphi} = \mathbb{Z}/p\mathbb{Z} \end{cases}$

- $\text{char } K = \min n$ (incluso lo 0) t.c. $n \cdot 1_K = 0_K$

$\begin{cases} \text{se char } K = p \Rightarrow \mathbb{Z}/_{p\mathbb{Z}} \hookrightarrow K \\ \text{se char } K = 0 \Rightarrow \mathbb{Z} \hookrightarrow K \Rightarrow \mathbb{Q} \hookrightarrow K \end{cases}$

$\begin{cases} \text{se char } K = 0 \Rightarrow K \geq \mathbb{Q} \\ \text{se char } K = p \Rightarrow K \geq \mathbb{Z}/_{p\mathbb{Z}} \cong \mathbb{F}_p \end{cases}$

- I campi finiti hanno char p

ESTENSIONI QUADRATICHE

- K campo, $\mathrm{char}\,K \neq 2$, L/K con $[L:K]=2$.
  Allora $\exists\ \alpha \in K$ t.c. $L = K(\sqrt{\alpha})$
  ovvero tutte le estensioni quadratiche si ottengono estraendo una radice quadrata

- K campo, $\mathrm{char}\,K \neq 2$, $\alpha, \beta \in K^* \Rightarrow K(\sqrt{\alpha}) = K(\sqrt{\beta}) \iff \alpha\beta \vee \alpha/\beta$ è un quadrato in K

- Se $\alpha \in (K^2)^*$ (cioè α è un quadrato) $\Rightarrow K(\sqrt{\alpha}) = K$. Pertanto se $K(\sqrt{\beta}) = K(\sqrt{\alpha}) \Rightarrow \beta \in (K^2)^* \Rightarrow \alpha\beta \in (K^2)^*$

- α, β due $\square \Rightarrow \alpha\beta$ è un quadrato, α, β non $\square \Rightarrow \alpha\beta\ \square$

LEMMA DEI GRADI DELLE ESTENSIONI

- K campo, $K(\alpha)$ e $K(\beta)$ due estensioni con $[K(\alpha):K] = m$ e $[K(\beta):K] = n$. Allora:
  1) $[K(\alpha,\beta):K] \leq m.n$
  2) Se $(m,n) = 1 \Rightarrow [K(\alpha,\beta):K] = m.n$.

- In generale $[m,n] \mid [K(\alpha,\beta):K] \Rightarrow [m,n] \leq [K(\alpha,\beta):K] \leq mn$

- Il grado del c.d.s è minore uguale di $n!$ dove $m = \deg(p(x))$

CAMPI FINITI

- F campo finito
  - $|F| < \infty$
  - $\mathrm{char}\,F = p$
  - $|F| = p^n$ se $\#F = p \Rightarrow F = \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$

- Se $f(x) \in \mathbb{F}_p[x]$ irrid. e $\deg f(x) = n$, allora $F = \dfrac{\mathbb{F}_p[x]}{(f(x))}$
  - $\mathrm{char}\,F = p$
  - $\#F = p^n$
  - F come sp. vett. su $\mathbb{F}_p$ è $\underset{\text{campo}}{F} \cong \mathbb{F}_p^n \cong \underset{\text{no campo}}{(\mathbb{Z}/p\mathbb{Z})^n}$
    l'iso vale solo se lo vedo come sp.v.

- $\mathbb{F}_p(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{F}_p[x],\ g(x) \neq 0 \right\}$
  $\hookrightarrow$ campo non finito di char p

- Binomio ingenuo $(x+y)^{p^n} = x^{p^n} + y^{p^n} \quad \forall n \in \mathbb{N}$

- Ogni sgr finito moltiplicativo di un campo è ciclico.
  $(\mathbb{F}_{p^n}^*, \cdot)$ è un gr. ciclico

- $\mathbb{F}_p^n$ è estensione semplice di $\mathbb{F}_p$, ovvero $\exists\ \alpha \in \mathbb{F}_{p^n}$ t.c. $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$

- Ogni generatore del gr. moltiplic. $\mathbb{F}_{p^n}^* = \langle \alpha \rangle$ è un generatore dell'estensione $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$
  il viceversa è falso. cioè se $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$ non è detto che α generi $\mathbb{F}_p^*$

- $\forall\ p$ primo $n \geq 1 \quad \exists\ f(x) \in \mathbb{F}_p[x]$ irrid con $\deg f(x) = n$.

- $\mathbb{F}_p[\alpha_1, \dots, \alpha_n] = \mathbb{F}_p[\alpha_i] = \mathbb{F}_{p^n}$

SOTTOCAMPI DI $\mathbb{F}_{p^n}$

- $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$

CAMPI DI SPEZZAMENTO SU $\mathbb{F}_p$

- $f(x) \in \mathbb{F}_p[x]$ $\quad f(x) = f_1^{e_1} \cdot \ldots \cdot f_n^{e_n}$ $\quad \deg(f_i) = d_i$

  $\Rightarrow$ c.d.s. di $f(x)$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ con $d = [d_1, \ldots, d_n]$

- $f(x) \in \mathbb{F}_p[x]$ irrid $\Rightarrow$ $f(x)$ ha radici multiple $\iff f'(x) = 0$

- Sia $f(x) \in \mathbb{F}_p[x]$ e $f'(x) = 0 \Rightarrow f(x) = (g(x))^p$ $\quad g(x) \in \mathbb{F}_p[x]$
  Nei campi finiti non succede che un pol. irriducibile abbia radici multiple
  Quindi i pol. irriducibili non hanno mai derivata nulla, poiché quelli che la hanno sono potenze p-esime

C.D.S di $x^n - 1$ su $\mathbb{F}_p$

- $f_n(x) = x^n - 1 \in \mathbb{F}_p[x]$ pol. ciclotomico $\quad n = p^a \cdot m \quad (m, p) = 1$
- $G_n = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^n - 1 = 0\} =:$ insieme delle radici n-esime di 1 nella chiusura algebrica del campo
- $G_n = G_m$. ed è ciclico di ord. m.
- $G_m \subseteq \mathbb{F}_{p^k} \iff m \mid p^k - 1$
- c.d.s di $f_n(x) = x^n - 1$ su $\mathbb{F}_p[x]$ è $\mathbb{F}_{p^k}$ $\quad k = \mathrm{ord}_m(p)$

ALTRO SULLE ESTENSIONI

- $L, M \subseteq \Omega$ sottocampi dello stesso campo Ω, abbiamo che il composto è $LM = L(M) = M(L)$ cioè il più piccolo sottocampo di Ω che contiene sia L che M.

  $L = K(\alpha_1, \ldots, \alpha_n)$ $\quad M = K(\beta_1, \ldots, \beta_m)$ $\quad LM = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$

Proprietà del composto

- $K \subset L \subset FL$ $\qquad K \subset F \subset FL$
  $[L:K] = m$ $\qquad [F:K] = n$

  $\Rightarrow [FL : K] = d < +\infty$

  $[m, n] \mid d$

SLOGAN

- Estensione finita $\Rightarrow$ algebrica   il viceversa è falso tranne quando l'est è semplice
- Un'est. L/K è alg se $\forall \alpha \in L$ α è alg su K
- campo delle estensioni algebriche
  L/K $A = \{\alpha \in L \mid \alpha$ è alg. su $K\}$
  - A è campo
  - A è est. alg di K
- est finit gen. $K(\alpha_1, \dots, \alpha_n) = \bigcap\limits_{\substack{K \subseteq M \subseteq L \\ \alpha_1, \dots, \alpha_n \in M}} M$
- est alg + finit gen $\Rightarrow$ finita
- Estensione è finita $\Leftrightarrow$ è finit gener da elt algebrici
- Proprietà delle estensioni algebriche rispetto a torri e composto
  1) $K \subset L \subset F$ F/K è alg $\Leftrightarrow$ F/L e L/K alg.
  2) L/K e M/K alg $\Leftrightarrow$ LM/K alg.

PROPRIETA' EST. FINITE

TORRI

$$\begin{tikzcd} L \arrow[d, dash, "<\infty"] \arrow[dd, bend right, dash, "<\infty"'] \\ F \arrow[d, dash, "<\infty"] \\ K \end{tikzcd}$$

L/K finita $\Leftrightarrow$ L/F e F/K finite

e $[L:K] = [L:F] \cdot [F:K]$

SHIFT

$$\begin{tikzcd} & LF \arrow[dl, dash] \arrow[dr, dash, "<\infty"] & \\ L \arrow[dr, dash, "<\infty"'] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

L/K finita $\Rightarrow$ LF/F finita

SHIFT + TORRI = COMPOSTO

$$\begin{tikzcd} & LF \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "<\infty"] & \\ L \arrow[dr, dash, "<\infty"'] & & F \arrow[dl, dash, "<\infty"] \\ & K & \end{tikzcd}$$

L/K , F/K finite $\Rightarrow$ LF/F finita

PROPRIETA' EST. ALGEBRICHE

TORRI

$$\begin{tikzcd} L \arrow[d, dash, "alg"] \arrow[dd, bend right, dash, "alg"'] \\ F \arrow[d, dash, "alg"] \\ K \end{tikzcd}$$

L/K alg $\Leftrightarrow$ L/F e F/K alg

SHIFT

$$\begin{tikzcd} & LF \arrow[dl, dash] \arrow[dr, dash, "alg"] & \\ L \arrow[dr, dash, "alg"'] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

L/K alg $\Rightarrow$ LF/F alg

SHIFT + TORRI = COMPOSTO

$$\begin{tikzcd} & LF \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "alg"] & \\ L \arrow[dr, dash, "alg"'] & & F \arrow[dl, dash, "alg"] \\ & K & \end{tikzcd}$$

L/K , F/K alg $\Leftrightarrow$ LF/F alg

ESTENSIONI

Problema: dato K campo, $\overline{K}$ chiusura alg., $\alpha \in \overline{K}$
in quanti modi si può immergere $K(\alpha)$ in $\overline{K}$ con
$\varphi: K(\alpha) \longrightarrow \overline{K}$ tc. $\varphi_{|K} = id_K$?

Proposizione 3.33 (Numero di estensioni via identità di $K(\alpha)$ a $\overline{K}$)
Dato un campo K ed $\alpha \in \overline{K}$, con $\overline{K}$ chiusura algebrica di K, detto k il numero di radici distinte di $\mu_\alpha(x)$ in $\overline{K}$, allora:

$$\exists \varphi_1, \dots, \varphi_k : K(\alpha) \hookrightarrow \overline{K} \qquad \text{con} \qquad \varphi_{i|K} = id_K$$

ovvero esistono esattamente k immersioni distinte da $K(\alpha)$ a $\overline{K}$, che estendono l'immersione di K in $\overline{K}$ per mezzo dell'identità.

Osservazioni

Tutte le estensioni da $K(\alpha) \longrightarrow \overline{K}$ sono tali che mandano α in un'altro radice del suo pol. minimo

PROBLEMA 2 $\longrightarrow$ Contare il numero di radici distinte di $\mu_\alpha(x)$ in $\overline{K}$

- criterio della derivata $\rightarrow (f, f') \neq 1 \Rightarrow$ ha radici multiple
- f irrid ha rad. mult. $\Leftrightarrow$ $f'(x) = 0$
- $f \in K[x]$, char $K = 0$ se f è irrid $\Rightarrow$ ha radici distinte
- $K = \mathbb{F}_{p^n} \Rightarrow$ ogni pol irrid ha derivata $\neq 0$

campo K tc. tutti i pol irrid in $K[x]$ hanno der. non nulla prende il nome di campo perfetto

Noi ci limiteremo ai campi perfetti pertanto un pol. irrid. di grado n avrà esatt. n radici distinte in $\overline{K}$

Proposizione 3.37 (Numero di estensioni di $K(\alpha)$ a $\overline{K}$)
Dato $\alpha \in \overline{K}$, con $[K(\alpha) : K] = n$, si ha che $\forall \varphi : K \hookrightarrow \overline{K}$ immersione, esistono esattamente n estensioni di φ ad una immersione da $K(\alpha)$ a $\overline{K}$, cioè:

$$\exists \varphi_1, \dots, \varphi_n : K(\alpha) \hookrightarrow \overline{K} \qquad \text{con} \qquad \varphi_{i|K} = \varphi$$

$\alpha \in \overline{K}$, coniugati di α su K sono le radici del pol min di α su K

$K \subset L$ separabile se il pol min è un pol sep. (ha radici tutte distinte)

ESTENSIONI NORMALI

F/K si dice normale se $\forall \varphi : F \hookrightarrow \overline{K}$ con $\varphi_K = id_K$ si ha che $\varphi(F) = F$

ovvero l'omo permuta gli elt che generano l'estensione con i loro coniugati ma rimangono nel campo

$\mathbb{Q}(\zeta_p)$ è est normale su $\mathbb{Q}$
$\mathbb{Q}(\sqrt[3]{2})$ non è normale su $\mathbb{Q}$

Proposizione 3.46 (Caratterizzazione delle estensioni normali)
Sia F/K un'estensione algebrica (finita)[a], sono fatti equivalenti:

(1) F/K normale.

(2) Ogni polinomio irriducibile $f(x) \in K[x]$ che ha una radice in F ha tutte le sue radici in F.

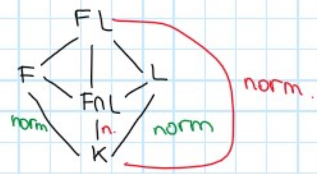
(3) F è il campo di spezzamento su K di una famiglia di polinomi di $K[x]$.

[a] La proposizione è vera anche senza questa ipotesi, ma la dimostriamo solo in questo caso.

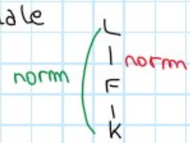
Ogni estensione di grado 2 e' normale

PROPRIETA' DELLE EST NORMALI RISPETTO AL COMPOSTO, $\cap$, TORRI

- F/K, L/K normali $\Rightarrow$ FL/K e $F\cap L/K$ sono normali



- $K \subset F \subset L$ se L/K è normale $\Rightarrow$ L/F è normale



non vale il viceversa

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ \big| \; 2 \text{ n.} \\ \mathbb{Q}(\sqrt{2}) \\ \big| \; 2 \text{ n} \\ \mathbb{Q} \end{array} \quad \text{non normale}$$

Gr. di Galois

E/K si dice estensione di Galois se è normale e separabile

$\{\varphi : E \hookrightarrow K \mid \varphi_{|K} = id_K\}$ si ha che $\varphi(E) = E$ perchè E/K normale

Per ogni φ restringo l'insieme di arrivo degli omo quindi il codominio

$Aut_K E = \{\varphi : E \xrightarrow{\sim} E \mid \varphi_{|K} = id_K\} =: K\text{-aut. di } E$

$Gal(E/K) := Aut_K E$ con $|Gal(E/K)| = [E:K]$

Oss

$f(x) \in K[x]$ irrid di grado n e F il suo cds su K. Allora

$n \mid [F:K] \mid n!$ e $Gal(F/K) \hookrightarrow S_n$ perchè $Gal(F/K) \curvearrowright \{$radici di $f(x)\}$

oss sull'azione

azione fedele e transitiva

$orb(\alpha_1) = \{\varphi(\alpha_1) \mid \varphi \in Gal(F/K)\} = \{\alpha_1, \dots, \alpha_n\}$ (ha un'unica orbita)

$\forall\, i = 1, \dots, n \quad \exists \quad \varphi_i : K(\alpha_1) \longrightarrow K(\alpha_i)$
$\qquad \alpha_1 \longrightarrow \alpha_i$

$L/K \quad \alpha \in L \quad \underbrace{K \subseteq K(\alpha)}_{\#\{\varphi(\alpha) \mid \varphi : L \to \bar{K} \;\; \varphi_{|K} = id\} = O(\alpha)} \subseteq L \qquad \mu_\alpha(x) = \prod_{\varphi(\alpha) \in O(\alpha)} (x - \varphi(\alpha))$

Gruppo di Gal di $\mathbb{F}_{q^d} / \mathbb{F}_q$

$\mathbb{F}_{q^d} / \mathbb{F}_q$ con $q = p^r$ è normale *

$\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ con $q = p^r$ è generato dall' autom. di Frobenius ϕ di $\mathbb{F}_{q^d}$

$$\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \phi \rangle \qquad \begin{aligned} \phi : \mathbb{F}_{q^d} &\longrightarrow \mathbb{F}_{q^d} \\ x &\longmapsto x^q \end{aligned}$$

Tutte le estensioni di campi finiti sono $\trianglelefteq$

$$\begin{array}{l} \mathbb{F}_{p^n} = \mathbb{F}_{q^d} \\ \quad | \ n \text{ per prop. Torri} \\ \mathbb{F}_{p^r} = \mathbb{F}_q \qquad * \, n \\ \quad | \ n \text{ per } * \\ \mathbb{F}_p \end{array}$$

Lez per.

Teorema dell' elt primitivo

K campo E/K finita (separabile) $\Rightarrow$ E/K è semplice cioè $\exists \, \gamma \in E$ t.c. $E = K(\gamma)$

Corr. di Galois

L/K di gal finita $\qquad H < \mathrm{Gal}(L/K)$

$$\begin{array}{c} L \\ | \\ L^H \end{array} \Big) \ \mathrm{Gal}(L/L^H) \cong H$$

- $L^H = \mathrm{Fix}(H) = \{ \alpha \in L \mid \varphi(\alpha) = \alpha \quad \forall \varphi \in H \} \subseteq L$

  =: sottocampo di L di tutti gli elt fissati da tutti i K-autom. di H ?

  $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L) = \{ \varphi : L \xrightarrow{\sim} L \mid \varphi_{|K} = id_K \}$

  $K \subseteq L^H \subseteq L \qquad\qquad H < \mathrm{Aut}_K(L)$

Lemma

- L/M di gal $\quad H \leq \mathrm{Gal}(L/M) \Rightarrow M = L^H \iff H = \mathrm{Gal}(L/M)$

  il campo fissato è quello base $\iff$ è fissato rispetto a tutto il gruppo

Lemma

L/K di gal $\quad H < \mathrm{Gal}(L/K)$ sia $\sigma \in \mathrm{Gal}(L/K) \Rightarrow L^{\sigma H \sigma^{-1}} = \sigma(L^H)$

$$\sigma(L^H) = \{ \sigma(\alpha) \mid \alpha \in L^H \} = \{ \sigma(\alpha) \mid \varphi(\alpha) = \alpha \ \forall \varphi \in H \}$$

Osservazione 3.68 — Non è detto che $\sigma(L^H)$ faccia L^H, tuttavia sarà sempre una sottoestensione di L/K, poiché L è ancora fissato, quindi in generale abbiamo:

$$\begin{tikzcd} & L \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\ L^H \arrow[dr, dash] & & \sigma(L^H) \arrow[dl, dash] \\ & K & \end{tikzcd}$$

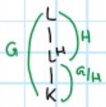
se fosse che $H \trianglelefteq G$, allora ovviamente avremmo $L^H = L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.

Teo CORRISPONDENZA DI GALOIS

L/K di Gal finita c'è una corr. biunivoca tra $\mathcal{E}_{L/K} = \{F \mid K \leq F \leq L\} \longleftrightarrow \mathcal{G} = \{H \mid H < G = \mathrm{Gal}(L/K)\}$
sottoest. di L/K — sgr di $\mathrm{Gal}(L/K)$

Inoltre $H \trianglelefteq G \iff L^H/K$ è normale

In tal caso $\underset{\substack{\| \\ G/H}}{\mathrm{Gal}(L^H/K)} \cong \dfrac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/L^H)} = \dfrac{G}{H}$



$\mathcal{E} \longleftrightarrow \mathcal{G}$

$F \xmapsto{\alpha} \mathrm{Gal}(L/F) < \mathrm{Gal}(L/K)$

$\underbrace{K \leq L^H \leq L}_{H}$ $\quad L^H \xleftarrow{\beta} H$

Schema dim

1) α e β sono una l'inversa dell'altra

2) $H \trianglelefteq G \iff \sigma H \sigma^{-1} = H \quad \forall \sigma \in \mathrm{Gal}(L/K) \iff \sigma L^H = L^{\sigma H \sigma^{-1}} = L^H \quad \forall \sigma \in \mathrm{Gal}(L/K)$

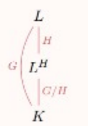
3) $\mathrm{res}\ \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L^H/K)$
$\sigma \longmapsto \sigma_{|L^H}$

$\mathrm{Ker\ res} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma_{|L^H} = id_{L^H}\} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in L^H\} = \mathrm{Gal}(L/L^H) \cong H$

$\{\varphi : L \longrightarrow L \text{ tc } \varphi_{|L^H} = id\}$
con $L \hookrightarrow E$
$L^H \hookrightarrow K$

$+$ 1° Teo omo

Esempio 3.70
Il teorema ci dice che, data ad esempio la torre:

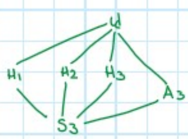


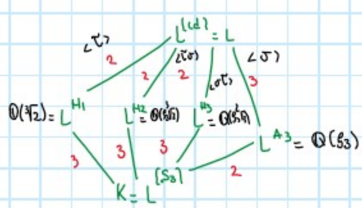
dove G è il gruppo di Galois di L/K, essendo anche L/L^H di Galois per ipotesi, e detto H il suo gruppo di Galois, allora se $H \triangleleft G$, si ha che anche L^H/K è di Galois ed il suo gruppo di Galois è G/H.

$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = L \qquad \mathbb{Q} = K$

$\mathrm{Gal}(L/K) \cong S_3$

sgr di S_3





$\sigma : \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2}$
$\zeta_3 \longmapsto \zeta_3$

$\tau : \sqrt[3]{2} \longmapsto \sqrt[3]{2}$
$\zeta_3 \longmapsto \zeta_3^2$

$\sigma\tau(\sqrt[3]{2}\zeta_3) = \sigma(\zeta_3^2\sqrt[3]{2}) = \sqrt[3]{2}$

$\tau\sigma(\sqrt[3]{2}\zeta_3) = \tau(\zeta_3^2\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}$

$\sigma\tau(\sqrt[3]{2}\zeta_3^2) = \sigma(\zeta_3\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2}$

Proprietà corr. di Galois

Proposizione 3.71 (Proprietà della corrispondenza di Galois)

Dati $H, S \leqslant \mathrm{Gal}\left({}^{L}\!/_{K}\right)$, allora valgono le seguenti:

(1) $H \leqslant S \iff L^H \supseteq L^S$.

(2) $L^{H \cap S} = L^H L^S$.[a]

(3) $L^{\langle S,H \rangle} = L^H \cap L^S$.

[a] Si intende il composto dei due campi.

$$\begin{tikzcd}
 & L \arrow[d, dash] & \\
 & L^H L^S = L^N \arrow[dl, dash] \arrow[dr, dash] & \\
L^H \arrow[dr, dash] & & L^S \arrow[dl, dash] \\
 & L^{H\cap S} \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Prop

L_1/K, L_2/K di Gal finite $\Rightarrow$ res: $\mathrm{Gal}(L_1L_2/K) \longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$

$$\sigma \longmapsto (\sigma_{|L_1}, \sigma_{|L_2})$$

res è inj

res è surj $\iff L_1 \cap L_2 = K$

Teorema 3.7

Per ogni primo p, l'estensione ${}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p}$ è normale e $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

Definizione 3.6. Dato p un numero primo, l'applicazione

$$\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} : x \longmapsto x^p$$

si dice **automorfismo di Frobenius**

Lemma 3.8

Dato K un campo, il polinomio $x^n - 1$ è separabile su K se e solo se $\mathrm{char}\, K \nmid n$.

Teorema 3.9

Sia $\zeta_n \in \mathbb{C}$ una radice primitiva n-esima dell'unità, allora l'estensione ${}^{\mathbb{Q}(\zeta_n)}\!/_{\mathbb{Q}}$ è normale e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.

Definizione 3.10 (Polinomio ciclotomico)**.** Data $\zeta_n \in \mathbb{C}$ una radice primitiva n-esima dell'unità, chiamiamo **n-esimo polinomio ciclotomico** il polinomio minimo $\Phi_n(x)$ di ζ_n su $\mathbb{Q}$.

Osservazione 3.11 — Poiché gli elementi di $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sono

$$\psi_k : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}} : \zeta_n \longmapsto \zeta_n^k$$

per $0 \leq k \leq n$, $(k,n) = 1$, possiamo scrivere $\Phi_n(x)$ come

$$\Phi_n(x) = \prod_{\substack{0 \leq k \leq n \\ (k,n)=1}} (x - \zeta_n^k)$$

Notiamo che le radici di $\Phi_n(x)$ sono tutte e sole le radici primitive n-esime dell'unità e che $\deg \Phi_n = \phi(n)$.

Proposizione 3.12

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

Proposizione 3.13
Siano ${}^{K}\!/_{F}$ un'estensione di Galois finita e ${}^{L}\!/_{F}$ un'estensione finita, allora

(1) ${}^{KL}\!/_{L}$ è un'estensione di Galois;

(2) $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$.

Dimostrazione. Consideriamo il seguente diagramma di campi, mostriamo i due enunciati separatamente

$$\begin{tikzcd}
 & KL \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] \arrow[ddr, dash] & & L \arrow[dl, dash] \arrow[ddl, dash] \\
 & K \cap L \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

Corollario 3.14
Siano ${}^{K}\!/_{F}$ un'estensione di Galois finita e ${}^{L}\!/_{F}$ un'estensione finita, se $K \cap L = F$ allora $[KL : F] = [K : F][L : F]$.

Dimostrazione. Consideriamo il seguente diagramma di campi

$$\begin{tikzcd} & KL \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\ K \arrow[dr, dash] & & L \arrow[dl, dash] \\ & F & \end{tikzcd}$$

per il Teorema delle Torri abbiamo $[KL : F] = [KL : L][L : F]$. Poiché $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L) = \mathrm{Gal}(K/F)$ per la Proposizione 3.13, in particolare $[KL : L] = [K : F]$, quindi $[KL : F] = [K : F][L : F]$. □

Proposizione 3.15
Siano ${}^{K_1}\!/_{F}$, ${}^{K_2}\!/_{F}$ estensioni di Galois finite, allora ${}^{K_1K_2}\!/_{F}$ è un'estensione di Galois. Inoltre:

(1) esiste un'immersione $\Phi : \mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$;

(2) $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ se e solo se $K_1 \cap K_2 = F$.

Proposizione 3.16
Sia $\zeta_n \in \overline{\mathbb{Q}}$ una radice primitiva n-esima di 1 per $n \geq 3$, allora $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$.

Osservazione 3.17 — In realtà vale che $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Infatti il polinomio $x^2 - \alpha x + 1$, con le notazioni di sopra, è un polinomio a coefficienti in $\mathbb{Q}(\alpha)$ che si annulla in ζ_n, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] \leq 2$. D'altra parte $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\alpha)$, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$ e quindi $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$.

Lemma 3.19

Dati p un primo e $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p, se $f(x)$ ha esattamente $p-2$ radici reali e 2 radici non reali e K è il suo campo di spezzamento su $\mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.

Lemma 3.20 (Lemma di Artin)

[a] Dato K un campo e G un sottogruppo finito di $\mathrm{Aut}(K)$, allora ${}^{K}\!/_{K^G}$ è un'estensione di Galois finita e $\mathrm{Gal}(K/K^G) = G$.

[a] La dimostrazione è da revisionare nella parte della dimostrazione della finitezza dell'estensione.

Teorema 3.22

Siano $p_1, \dots, p_n \in \mathbb{Z}$ primi distinti, poniamo $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. ${}^{K_n}\!/_{\mathbb{Q}}$ è un'estensione di Galois e $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$.

Teorema 3.25

Siano $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ un polinomio irriducibile, definiamo $\Delta = a^2 - 4b$. Posto K il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ si ha:

(1) se $\sqrt{b} \notin \mathbb{Q}$ e $\sqrt{b\Delta} \notin \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$;

(2) se $\sqrt{b} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(3) se $\sqrt{b\Delta} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$;

Teorema 3.29

Dato p un primo dispari, l'unica sottoestensione di $\mathbb{Q}(\zeta_p)$ quadratica su $\mathbb{Q}$ è

(1) $\mathbb{Q}(\sqrt{p})$ se $p \equiv 1 \pmod 4$;

(2) $\mathbb{Q}(\sqrt{-p})$ se $p \equiv 3 \pmod 4$.