

- Siano $\alpha_1, \dots, \alpha_n \in L$: voglio definire $K(\alpha_1, \dots, \alpha_n)$

① Il più piccolo sottocampo di L che contiene di K e K

② $\bigcap_{K \subset F \subset L, \alpha_i \in F} F$ ben definito : unicamente L rispetto

③ Procedimento induttivo : $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$

④ $\left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in K[x] \right\}$

In generale considero K campo, L/K estensione e $S \subset L$: $K(S)$

① $\bigcap_{K \subset F \subset L, S \subset F} F$

② $\bigcup_{S \cap S' \subset S, S' \in \mathcal{N}} K(S')$

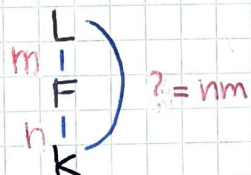
IO $\nearrow$ $K \subset F, S \subset F \rightarrow K(S \cap S') \subset F$ IN $\nwarrow$ contro

Es: $\mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$: $S = \{\sqrt{p}\}$

Def: $F, K \subset L \rightarrow KF = K(F) = F(K)$

* PROPRIETA' ESTENSIONI FINITE

① TORRI :

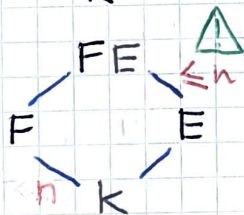


L/K finita $\Leftrightarrow L/F$ e F/K finite

$\{v_i\}$ di F/K , $\{w_j\}$ di L/F
 $\rightarrow \{v_i w_j\}$ base di L/K .

② SHIFT:

$F, E \subset L$



$[F:K] = n \Rightarrow [FE:E] \leq n$

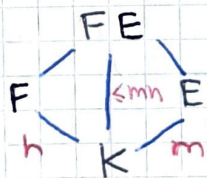
Sia $\{v_1, \dots, v_n\}$ K -base di F :
 considero $\alpha \in FE = E(F)$:

$$\alpha = \sum_{i=1}^n e_i f_i = \sum_{i=1}^n e_i \sum_{j=1}^{n_i} k_{j,i} v_j$$

$\rightarrow \alpha$ si scrive come comb lineari di $\{v_j\}$
 a coeff in E

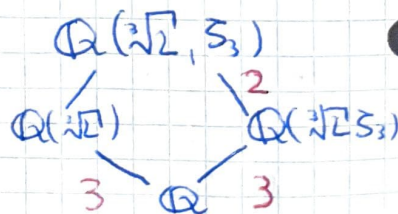
③ COMPOSTO:

$F, E \subset L$



$[1+2 \Rightarrow 3 \text{ sempre}]$

Es: $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$, $E = \mathbb{Q}(\zeta_3 \sqrt[3]{2})$



Teo 1: L/K finita $\Rightarrow L/K$ algebrica

Dim: $n = [L:K]$, sia $\alpha \in L$: $\underbrace{1, \alpha, \dots, \alpha^n}_{n+1 \text{ el di } L}$ linearmente dipendenti in K

Oss: algebrica $\nRightarrow$ finita

es: $\mathbb{Q}(\{\sqrt[n]{2} \mid n \geq 1\}) = K$.

- $K/\mathbb{Q}$ algebrica (.)
- $K/\mathbb{Q}$ non è finita: contiene estensioni di grado arbitr. grande: $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$

Teo 2: L/K finita $\Leftrightarrow L/K$ algebrica e finitamente generata

Dim: $(\Rightarrow)$ ok algebrica, ma $L = \langle v_1, \dots, v_n \rangle_K = K(v_1, \dots, v_n) \checkmark$
 $(\Leftarrow)$ $L = K(\alpha_1, \dots, \alpha_n)$ considero $L_i = K(v_1, \dots, v_i)$

$K = L_0 \subset L_1 \subset \dots \subset L_{n-1} \subset L_n$ e $L_{i+1} = L_i(v_{i+1})$
 ognuna di queste è FINITA $\uparrow$
 [v_i algebrico in L_i ed estensioni semplici] $\rightarrow$ TORRI: finita

Cor 1: E/K estensori e $F = \{e \in E \mid e \text{ algebrico in } K\}$

$\Rightarrow F$ è un campo e F/K è algebrico

Dim: $\alpha, \beta \in F$: $K(\alpha, \beta)$ è finita su $K \rightarrow$ algebrica su K

$\Rightarrow \alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K(\alpha, \beta)$ [quindi sono algebrici e stanno in F]

Cor 2: L/K algebrica $\Leftrightarrow L$ è generata su K da elementi algebrici
 [algebricamente generata]

questo dimostra (.)

Dim: L/K algebrica $\Rightarrow L = K(L) \checkmark$

$L = K(S)$ e $\forall s \in S$ sia s algebrico in K .

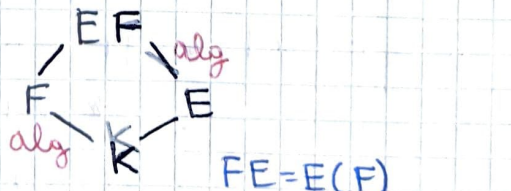
Considero $F = \{x \in L \mid x \text{ algebrico in } K\}$ $\begin{matrix} \text{campo} \\ \text{algebrico in } K \end{matrix}$
 $\rightarrow K \subset F \subset L = K(S)$ e $S \subset F \rightarrow F = L$

* PROPRIETÀ DELLE ESTENSIONI ALGEBRICHE

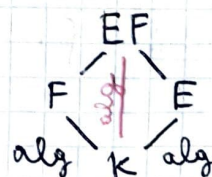
① TORRI



② SHIFT



③ COMPOSTO 1+2



$\alpha \in E$: $p_\alpha(x) \in K(\text{coef di } p_\alpha)[x]$
 $K_1(\alpha) = K_1 \xrightarrow{\text{alg + f.g. FINITA}} K$ FINITA $\Rightarrow$ alg

$\rightarrow$ alg in E

Def.: Ω campo: si dice Ω **ALGEBRICAMENTE CHIUSO** se
 $\forall f \in \Omega[x] - \Omega, f$ ammette una radice in Ω .

$\equiv$ • Gli unici pol. irriducibili di $\Omega[x]$ sono quelli di grado 1

$\equiv$ • $\forall f \in \Omega[x] - \Omega, f$ si spezza in $\Omega[x]$ come prodotto di fattori lineari

Teo [Fondamentale dell'Algebra] $\mathbb{C}$ algebricamente chiuso

Def.: K campo, $\bar{K}$ è una chiusura algebrica di K se:

- $\bar{K}$ è algebricamente chiuso
- $\bar{K}$ algebrico su K

Esempio: • $\mathbb{C} = \overline{\mathbb{R}}$ perché

- $\mathbb{C}$ alg. chiuso
- $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

• $\mathbb{C} \neq \bar{\mathbb{Q}}$ ($\mathbb{C}$ non algebrico su $\mathbb{Q}$)

Teorema: Dato un campo K esiste sempre una sua chiusura algebrica. Inoltre due chiusure algebriche di K sono isomorfe su K
 $\hookrightarrow$ con un isomorfismo su K puntualmente

Esempio: • $\bar{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q} \}$ è un campo, ed è algebrico su $\mathbb{Q}$ per costruzione

Dimostriamo che $\bar{\mathbb{Q}}$ è algebricamente chiuso:

sia $f \in \bar{\mathbb{Q}}[x] : \alpha \in \mathbb{C}$ radice di f

Oss: $K = \mathbb{Q}(\text{coeff. di } f) : \mathbb{Q} \xrightarrow[\text{FIN + F.G.}]{\text{alg}} K \xrightarrow[\text{FIN + F.G.}]{\text{alg}} K(\alpha)$

$\rightarrow \alpha$ algebrico su $\mathbb{Q} : \alpha \in \bar{\mathbb{Q}}$

Questo esempio si generalizza al caso in cui $K \subset \Omega$ alg. chiuso
 definisco $\bar{K} = \{ \alpha \in \Omega \mid \alpha \text{ è algebrico su } K \}$

$\Rightarrow \bar{K}$ chiusura algebrica di K

Se non conosco $K \subset \Omega$ algebricamente chiuso procedo con:

Oss: $f \in K[x]$ e $g \mid f$, g irriducibile in $K[x]$

$\Rightarrow f$ ha almeno una radice in $K[x]/(g)$

Oss 2: $f_1, \dots, f_n \in K[x]$ e g_1 fattore irriducibile di f_1 in $K[x]$

$\rightarrow K_1 = K[x]/(g_1)$

g_2 fattore irriducibile di f_2 in $K_1[x]$

$\rightarrow K_2 = K_1[x]/(g_2)$

$\Rightarrow$ Trovo K_n in cui tutti gli f_i si fattorizzano (.)

Dim: [Artin]

Idea: aggiungere in un solo passo una radice di ogni pol. di $K[x]$

• Sia $\Lambda^* = \{p(x) \mid \deg p \geq 1, p(x) \in K[x]\} = \{p_\lambda(x)\}_{\lambda \in \Lambda}$

Per ogni p_λ sia x_λ indeterminata e consideriamo $X = \{x_\lambda\}_{\lambda \in \Lambda}$

$\Rightarrow$ considero in $K[X]$ l'ideale $I = \langle p_\lambda(x_\lambda) \mid \lambda \in \Lambda \rangle$

Oss: $1 \notin I$. Infatti se $1 = \sum_{i=1}^n f_{\lambda_i}(x) p_{\lambda_i}(x_{\lambda_i})$

allora costruisco: $\varphi: K[X] \longrightarrow K'$ ← campo costruito
minimo che contenga
le radici di
 $\{p_{\lambda_i}\}_{i=1}^n$

1	$\mapsto$	1
x_{λ_i}	$\mapsto$	α_i
x_λ	$\mapsto$	0

Ma allora $1 = \varphi(1) = \varphi(\sum f_{\lambda_i}(x) p_{\lambda_i}(x_{\lambda_i})) = \sum f_{\lambda_i}(x) \cdot \underbrace{p_{\lambda_i}(\alpha_i)}_{=0} = 0$, ass.

Quindi I è un ideale proprio: $\exists \mathcal{M}$ ideale max di $K[X]$
tale che $I \subset \mathcal{M}$

$\Rightarrow E_1 = K[X]_{/\mathcal{M}}$ è un campo e $K \subset E_1$ $[K \rightarrow K[X] \rightarrow E_1]$

$\Rightarrow E_1 = K[\{\bar{x}_\lambda\}_{\lambda \in \Lambda}]$ Oss: $\bullet E_1$ contiene le radici di
tutti i polynomi con coeff in K
 $\bullet E_1$ alg generato su K

Possiamo quindi costruire

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \dots$$

e considerare $\Omega = \bigcup_{n \geq 1} E_n$: dimostro che Ω è alg. chiuso

sia $p(x) \in \Omega[x] \setminus \Omega$:

$\exists m$ t.c. $p(x) \in E_m[x] \rightarrow p(x)$ ha una radice in E_{m+1}
 $\Rightarrow p(x)$ ha una radice in Ω

$\rightarrow$ quindi $K \subset \Omega$ algebricamente chiuso.

Inoltre E_i è algebrico su $E_{i-1} \rightarrow \Omega$ algebrico su K

Esempio: $\bullet \mathbb{F}_p$: esiste $\overline{\mathbb{F}_p}$ su $\uparrow$. $\mathbb{F}_{p^n} = \{ \alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha \}$
e voglio dimostrare che $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

È ovvio che $\overline{\mathbb{F}_p} \supset \bigcup_{n \geq 1} \mathbb{F}_{p^n}$. Basterà che io faccio vedere
che $\bigcup_n \mathbb{F}_{p^n}$ è algebricamente chiuso.

Sia $f \in \bigcup_{n \geq 1} \mathbb{F}_{p^n}[x] \Rightarrow f \in \mathbb{F}_{p^d}[x]$ e quindi le radici di f
sono in una estensione finita di $\mathbb{F}_{p^d}$.

Manca da dimostrare l'unicità di $\bar{K}$ a meno di isomorfismo

• ESTENSIONI DI OMONORFISMI

L/K , $\varphi: K \rightarrow F \subset \bar{K}$: si può estendere φ ad L ?
in quanti modi?

Caso $L = K[\alpha]$: $L = K[x]/(p_\alpha(x))$ estendere φ ad L
equivale a cercare

$$\tilde{\varphi}: K[x] \rightarrow F \quad \text{t.c.} \quad \begin{matrix} \ker(\tilde{\varphi}) = (p_\alpha(x)) \\ \tilde{\varphi}|_K = \varphi \end{matrix}$$

$$\Rightarrow \tilde{\varphi}(p_\alpha(x)) = \tilde{\varphi}(\sum a_i x^i) = \sum \varphi(a_i) \beta^i = 0$$

se e soltanto se β è una radice di $\varphi(p_\alpha)$

$\Rightarrow$ posso estendere φ a L in $\frac{\# \text{radici distinte di } \varphi(p_\alpha) \text{ in } F}{\# \text{radici distinte di } p_\alpha \text{ in } F}$ modi

Teo: $\varphi: K \rightarrow \bar{K}$, F/K algebrica $\Rightarrow$ esiste un'estensione di φ a F ovvero
 $\exists \tilde{\varphi}: F \rightarrow \bar{K}$ t.c. $\tilde{\varphi}|_K = \varphi$.

$$\text{Dim: } X = \{ (E, \psi) : K \subset E \subset F, \psi: E \rightarrow \bar{K}, \psi|_K = \varphi \} \ni (K, \varphi)$$

Osserviamo che, data la relazione $(E_1, \psi_1) \preceq (E_2, \psi_2)$
se $E_1 \subset E_2$ e $\psi_2|_{E_1} = \psi_1$.

X è iniettivo (ricordo!), ovvero per ogni catena

$$(E_1, \psi_1) \preceq (E_2, \psi_2) \preceq \dots \quad \text{in } X \text{ ammette come maggiorante} \\ (U E_i, \psi) \quad \text{con } \psi(\alpha) = \psi_j(\alpha) \quad \text{t.c. } \alpha \in E_j$$

$\rightarrow$ Per Zorn esiste (F_0, ψ_0) massimale in X

Claim: $F_0 = F$ se $F_0 \subsetneq F$: $\alpha \in F \setminus F_0$ ed estendo ψ_0
a $\tilde{\psi}_0: F_0(\alpha) \rightarrow \bar{K}$

$$\rightarrow (F_0, \psi_0) \preceq (F_0(\alpha), \tilde{\psi}_0) \in X$$

Dim (Unicità della chiusura algebrica):

supponiamo che $\bar{K}$ e Ω chiusure algebriche di K :

$$\varphi: K \hookrightarrow \bar{K} \xrightarrow{\text{univ. prima}} \text{ si estende a } \tilde{\varphi}: \Omega \rightarrow \bar{K} \quad \text{t.c. } \tilde{\varphi}|_K = \varphi$$

Voglio dimostrare che $\tilde{\varphi}$ è un isomorfismo:

- $\tilde{\varphi}$ è iniettivo (non è nullo)

- Quando $\tilde{\varphi}(\Omega) \subset \bar{K}$: dico che $\tilde{\varphi}(\Omega)$ è algebricamente chiuso
sia $f \in \tilde{\varphi}(\Omega)[x] \Rightarrow f = \tilde{\varphi}g$ con $g \in \Omega[x]$

$$\text{ovvero } \exists \alpha \in \Omega : g(\alpha) = 0 \Rightarrow f(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(g(\alpha)) = 0$$

$$\rightarrow K \subset \varphi \Omega \subset \bar{K} \leftarrow \alpha \in \bar{K} \text{ algebrico su } K \rightarrow \exists \tilde{\varphi} \Omega \} \bar{K} = \tilde{\varphi} \Omega$$

alg. chiuso $\Rightarrow \alpha \in \tilde{\varphi} \Omega$

Esercizio: se K è un campo infinito $\Rightarrow |\bar{K}| = |K|$

- Comma $A_n = \{ \alpha \in \bar{K} \mid [K(\alpha) : K] \leq n \}$: $\bar{K} = \bigcup_n A_n$

• Osservo che $|K[x]_{\leq n}| = |K^{n+1}| = |K|$ ed inoltre

$$A_n \xrightarrow{\alpha} K[x]_{\leq n} \xrightarrow{p_n(x)} \text{e a fibra limitata}$$

(la pre-immagine di ogni α è finito)

$$\rightarrow |A_n| = |K[x]_{\leq n}| = |K|$$

$$\Rightarrow |\bar{K}| = \lim_n |A_n| = |K|$$

03/07

$\rightarrow \varphi_0 : K \rightarrow \bar{K}$ si estende a $\varphi : K(\alpha) \rightarrow \bar{K}$ t.c. $\varphi|_K = \varphi_0$

in d modi dove $d = \# \text{ radici distinte di } p_\alpha(x)$

$\rightarrow$ se $f(x)$ ha m radici distinte in $\bar{K}$, $f(x)$ ha m radici distinte in ogni chiusura algebrica di K .

Def: K campo, $f(x) \in K[x]$ di grado > 1 .
Si dice campo di spezzamento di f su K (in $\bar{K}$) e definito da $L = K(\alpha_1, \dots, \alpha_n)$ dove $\{\alpha_1, \dots, \alpha_n\}$ è l'insieme delle radici di $f(x)$ in $\bar{K}$

Oss 1: L è il più piccolo sotto campo di $\bar{K}$ che contiene K in cui f si spezza come prodotto di fattori lineari.

Oss 2: L è univocamente determinato (fissate la chiusura algebrica)

Def: $\mathcal{F} = \{f_i\}_{i \in I}$ con $f_i \in K[x]$, $\deg f_i \geq 1$. Allora il campo di spezzamento di $\mathcal{F}$ su K (in $\bar{K}$) è

$$L = K(\{\alpha_{ij}\}_{i \in I, j=1, \dots, n_i})$$

• dove $\{\alpha_{ij}\}_{j=1, \dots, n_i}$ sono le radici di f_i in $\bar{K}$.

$$\equiv L = \prod L_i \text{ dove } L_i \text{ è il C&S di } f_i$$

$$\equiv L = K(\cup L_i)$$

$$\equiv L = \bigcup_{i \in I} L_{i \in I} \text{ con } L_{i \in I} = \prod_{i \in I \cap I_i} L_i$$

Prop: L, L' C&S di $\mathcal{F}$ su $K \Rightarrow \forall \sigma : L \rightarrow \bar{L}$ con $\sigma|_K = \text{id}$, si ha $\sigma L = L'$

Questo mi dice che $L \cong L'$ e che l'unico sottocampo di $\bar{L}$ isomorfo a L è L' .

Dim: $\bullet \mathcal{F} = \{f\} \rightarrow L = K(\alpha_1, \dots, \alpha_n)$ e $f(x) = \prod (x - \alpha_i)$ non nec. distinta allora

$$f = \sigma f = \prod (x - \sigma(\alpha_i)) \text{ in } \bar{L}$$

Ma allora in $\bar{L}$ le radici di f sono $\{\sigma(\alpha_i)\}$

$$\Rightarrow L' = K(\sigma \alpha_1, \dots, \sigma \alpha_n) = \sigma L$$

$$\bullet \mathcal{F} \text{ qualsiasi} = \{f_i\}_{i \in I} \Rightarrow L = \prod_{i \in I} L_i \text{ e } L' = \prod_{i \in I} L'_i \text{ e } \sigma L_i = L'_i \text{ (1)} \\ \Rightarrow \sigma L = L'$$

Cor: L, L' campi di spezzamento di f su K : $L \cong L'$ e se $L = L' \rightarrow \bar{L} = \bar{L}'$

* ESTENSIONI NORMALI

Def: F/K algebrica, si dice NORMALE se $\forall \varphi: F \rightarrow \bar{F}, \varphi|_K = \text{id} \Rightarrow \varphi F = F$

Es: $\mathbb{Q}(\sqrt[3]{2})$ e $\varphi: \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q} + i.c.$ $\varphi|_{\mathbb{Q}} = \text{id}$
se $\varphi(\sqrt[3]{2}) = \sqrt[3]{2} \xi_3 \Rightarrow \varphi(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2} \xi_3) \rightarrow \mathbb{Q}(\sqrt[3]{2})$ non normale

Prop: F/K algebrica e $\varphi: F \rightarrow \bar{K}$: $\varphi|_K = \text{id}$

se $\varphi F \subseteq F \Rightarrow \varphi F = F$

Dim: Caso F/K finito $K \subseteq \varphi F \subseteq F$ e $[F:K] = [\varphi F: \varphi K]$

$\rightarrow \varphi F = F$

Caso generale

$\varphi F \subseteq F$: sia $\alpha \in F$, $p_\alpha(x) \in K[x]$ pol. min di α su K
 $\rightarrow p_\alpha$ ha radici $\alpha = \alpha_1, \dots, \alpha_d$ in F

$\Rightarrow F_0 = K(\alpha_1, \dots, \alpha_d)$ e $\varphi F_0 \subseteq F_0$
poiché $\varphi(\alpha_i) \in F$ $\forall i$ ed α radice di $\varphi(p_\alpha(x)) = p_\alpha$

ma $[F_0:K]$ è finita $\rightarrow \varphi F_0 = F_0$

Ma allora $\alpha \in F_0 = \varphi F_0 \subseteq \varphi F \rightarrow \alpha \in \varphi F$ $F \subseteq \varphi F$

Teo: F/K algebrico. Sono fatti equivalenti:

① F/K è normale

② $\forall f \in K[x]$ IRRIDUCIBILE: se f ha una radice in F
 $\Rightarrow f$ si spezza completamente su F

③ F è il cds di una famiglia di polinomi di $K[x]$

Dim: 1 $\Rightarrow$ 2 $f = p_\alpha(x)$ con $\alpha \in F$: sia $\beta \in \bar{F}$ radice di f .

Considero $\varphi: K(\alpha) \rightarrow K(\beta)$ $\varphi|_K = \text{id}$
 $\alpha \mapsto \beta$

$\Rightarrow$ posso estendere φ a una immersione $\bar{\varphi}: F \rightarrow \bar{F}$: $\bar{\varphi}|_{K(\alpha)} = \varphi$

Poiché $\bar{\varphi}|_K = \varphi|_K = \text{id}$ e F/K è normale: $\bar{\varphi} F = F$
ma allora $\bar{\varphi}(\alpha) = \varphi(\alpha) = \beta \in F$.

Quindi $\forall \beta \in \bar{F}$ radice di $f \rightarrow \beta \in F$.

2 $\Rightarrow$ 3 Scelgo $\mathcal{J} = \{ p_\alpha(x) \mid \alpha \in F \}$ e sia $L = \text{cds di } \mathcal{J} \text{ su } K$

È chiaro che $F \subseteq L$, d'altra parte il cds di $p_\alpha \in F \forall \alpha \in F$
ovvero $L \subseteq F$

3 $\Rightarrow$ 1 $F = K(\{\alpha_{ij}\}_{i \in I, j=1, \dots, n_i})$ e sia $\varphi: F \rightarrow \bar{F}$: $\varphi|_K = \text{id}$
 $\Rightarrow \forall \alpha_{ij}$: $\varphi(\alpha_{ij}) = \alpha_{ij, c_{ij}} \Rightarrow \varphi F = K(\{\alpha_{ij, c_{ij}}\}_{i \in I, j=1, \dots, n_i}) = F$

Esempi • $\mathbb{Q}(\{\sqrt{n} \mid n \in \mathbb{N}\})$ c.d.s di $\mathcal{F} = \{x^2 - m \mid m \in \mathbb{Z}\}$: normale su $\mathbb{Q}$
 • $\mathbb{Q}(\{\zeta_m \mid m \geq 1\})/\mathbb{Q}$ c.d.s di tutti i ciclotomici : normale su $\mathbb{Q}$
 $\mathbb{Q}^{ab}$

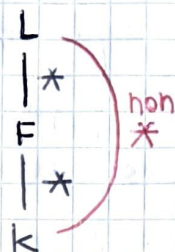
* PROPRIETA' DELLE ESTENSIONI NORMALI

① TORRI



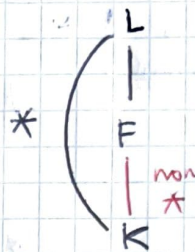
$$\varphi: L \rightarrow \bar{K} : \varphi|_F = \text{id} \\ \Rightarrow \varphi|_K = \text{id} \rightarrow \varphi L = L$$

L/K Norm



$$L = \mathbb{Q}(\sqrt[4]{2}) \\ K = \mathbb{Q}(\sqrt{2}) \\ K = \mathbb{Q}$$

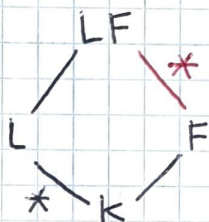
ma $x^4 - 2$ irr. non
 ha tutte le sue radici
 $\in L$, $\sqrt{2} i \notin L$



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

$\rightarrow F/K$ non è normale
 ma L/K lo è.

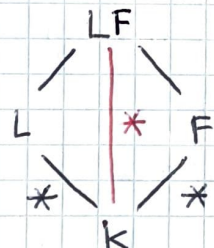
② SHIFT



$$\varphi: LF \rightarrow \bar{K} : \varphi|_F = \text{id} \rightarrow \varphi|_K = \text{id} \rightarrow \varphi L = L \\ \text{quindi } \varphi LF = \varphi(F(L)) = F(\varphi(L)) = FL$$

$\varphi|_F = \text{id}$

③ COMPOSTO



$$\varphi: LF \rightarrow \bar{K} : \varphi|_K = \text{id}$$

ma allora:

$$- L/K \text{ norm.} : \varphi L = L \\ - F/K \text{ norm.} : \varphi F = F \rightarrow \varphi LF = LF$$

e $L \cap F/K$ norm.

[e più tardi @ anche $LF/F \cap L$ norm]

$$\varphi: L \cap F \rightarrow \bar{K} \rightarrow \bar{\varphi}: LF \rightarrow \bar{K} \\ \text{con } \varphi L = L, \varphi F = F \\ \varphi(L \cap F) = L \cap F$$

Def: Data F/K si dice chiusura normale di F/K il più piccolo campo $F \subset L \subset \bar{F}$ t.c. L/K è normale

(ben definito: $\mathcal{J} = \{F \subset L \subset \bar{F} \mid L/K \text{ norm}\} \ni \bar{F}$ e $L = \bigcap_{J \in \mathcal{J}} J$)

$$\text{Equivalentemente: } \mathcal{I} = \{\varphi: F \rightarrow \bar{F} \mid \varphi|_K = \text{id}\} \rightarrow \tilde{F} = \prod_{\varphi \in \mathcal{I}} \varphi F$$

è la CHIUSURA NORMALE di F/K

Prop: ① Le due def. sono equivalenti, ovvero $\tilde{F}$ è la minima estensione normale che contiene F

$$② [F:K] < +\infty \Rightarrow [\tilde{F}:K] < +\infty$$

Dim: Per dimostrare ① devo dimostrare due cose:

1. $\tilde{F}/K$ è normale: $\varphi: \tilde{F} \rightarrow \tilde{F}$ $\varphi|_K = \text{id}$, voglio $\varphi\tilde{F} \subset \tilde{F}$
 per def: $\tilde{F} = \bigcup_{\sigma \in \mathcal{I}} \sigma F$: $\varphi(\sigma F) = (\varphi\sigma)F \subset \tilde{F}$
 $\Rightarrow \varphi\tilde{F} \subset \tilde{F}$
 con $\varphi\sigma|_K = \text{id}$
 $\Rightarrow \varphi\sigma \in \mathcal{I}$

2. $\tilde{F}$ è la più piccola sottoestensione normale che contiene F | Sia $L \supset F$: L/K normale, voglio $\tilde{F} \subset L$
 $\forall \sigma \in \mathcal{I}$: estendo σ a $\tilde{\sigma}: L \rightarrow \tilde{F}$: $\tilde{\sigma}|_F = \sigma$
 L/K normale: $\tilde{\sigma}L = L$ ma $\sigma F \subset \tilde{\sigma}L = L$
 $\rightarrow \tilde{F} = \bigcup_{\sigma \in \mathcal{I}} \sigma F \subset L$

Dimostriamo ②: supponiamo $[F:L] = n \in \mathbb{N} \rightarrow F = K(d_1, \dots, d_n)$
 Ma quindi $\forall \varphi: F \rightarrow \bar{K}$: $\varphi(d_i) = \beta_i$ radice di $p(d_i)(x)$
 $\Rightarrow \tilde{F}$ è il CdS di $\{p_{d_1}, \dots, p_{d_n}\} \rightarrow \text{FIN. GENERATO}$

* ESTENSIONI SEPERABILI

03/12

Def: $f(x) \in K[x]$ si dice separabile se in $\bar{K}$ ha tutte le radici distinte
 es: $(x-1)^2$ non è separabile

[Criterio della derivata] f ha radici multiple $\Leftrightarrow (f, f') \neq 1$

Dim: $f(\alpha) = 0$ con $\alpha \in \bar{K} \rightarrow f(x) = (x-\alpha)g(x)$
 quindi $f'(x) = g(x) + (x-\alpha)g'(x)$

$\Rightarrow f'(\alpha) = 0 \Leftrightarrow g(\alpha) = 0 \Leftrightarrow x-\alpha \mid g(x)$

Quindi: f inducibile $\rightarrow f$ non è separabile $\Leftrightarrow f' \equiv 0$

a meno di invertibili;
 e polinomio minimo delle sue radici } $f(\alpha) = 0 \Rightarrow \forall g: g(\alpha) = 0, f \nmid g$

Ma poi che f non separabile $\Leftrightarrow (f, f') \neq 1$ e $\deg f' < \deg f \rightarrow f' \equiv 0$

Lemma: $f \in K[x]$ inducibile.

- se $\text{char } K = 0 \Rightarrow f$ è separabile
- se $\text{char } K = p$: sia r il max naturale t.c. f è un polinomio in x^{p^r}
 $[f(x) = g(x^{p^r})]$ allora g è inducibile, separabile
 e ogni radice di f ha molteplicità p^r ed è
 radice p^r -esima di uno zero di g .

Dim: • $\text{char } K = 0$: f inducibile e $\deg f \geq 1 \rightarrow \deg f' = \deg f - 1 \geq 0 \checkmark$

• $\text{char } K = p$: $f(x) = \sum_{i=0}^n a_i x^i$: $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$

Quindi $f'(x) = 0 \Leftrightarrow i a_i \equiv 0 \pmod{p} \Leftrightarrow \begin{cases} a_i \equiv 0 \pmod{p} \\ i \equiv 0 \pmod{p} \end{cases}$

* $f' \neq 0$: $r=0$ e la tesi è vera

* $f' = 0$: $r \geq 1 \rightarrow$ scelgo r max e $f(x) = g(x^{p^r})$
 esiste perché f ha deg finito

- Voglio mostrare che g è irriducibile e separabile
- g irriducibile (dc) ($\neq$ inducibile)
 - g separabile: $g(x) = \sum_{\substack{i=0(p) \\ 1 \leq i \leq n}} a_i x^{ip^r} \rightarrow g'(x) = \sum \frac{ia_r}{p^r} x^{i-1}$

ma per massimalità di $r \nexists i: p^{r+1} \nmid i: g' \neq 0$

$$\rightarrow g(x) = \prod_{i=1}^k (x - \alpha_i) \text{ con } \alpha_i \in \bar{K}: \alpha_i \neq \alpha_j$$

$$\text{E quindi } f(x) = \prod_{i=1}^k (x^{p^r} - \alpha_i) = \prod_{i=1}^k (x^{p^r} - \beta_i^{p^r}) = \prod_{i=1}^k (x - \beta_i)^p$$

$\exists \beta_i \in \bar{K}: \alpha_i = \beta_i^{p^r}$ $\text{char } K = p$

- Def:
- $\alpha \in \bar{K}$ si dice separabile su K se $\mu_\alpha(x)$ è separabile.
 - L/K si dice separabile se $\forall \alpha \in L, \alpha$ è separabile su K .
 - K si dice perfetto se ogni sua estensione algebrica è separabile.

Oss: Se $\text{char } K = 0 \Rightarrow K$ è perfetto

Oss2: $\mathbb{F}_p^n$ è perfetto: in fatti dato $f \in \mathbb{F}_p[x]$ non separabile

$$\rightarrow f(x) = h(x^p) \stackrel{\alpha^p \equiv a}{=} h(x)^p \text{ quindi } f \text{ non irriducibile}$$

$\Rightarrow$ Ogni estensione di $\mathbb{F}_p$ è separabile, quindi anche ogni estensione di $\mathbb{F}_p^n$.

esempio: $f(x) \in \mathbb{F}_p(t)[x]: f(x) = x^p - t$ dimostro che è IRRIDUCIBILE e NON SEPARABILE

aiuti:

- $\mathbb{F}_p(t)[x] / (x^p - t) = K: \mathbb{F}_p(t)[x]$ non separabile

- $\mathbb{F}_p(t)[x]$ non è perfetto

Dim: $\circ f'(x) = p x^{p-1} \equiv 0$

$\circ$ Inoltre guardo $f(x) = x^p - t$ in $\mathbb{F}_p[t][x]$

Osservo che $P=(t) \in \mathbb{F}_p[t]$ è primo e $x^p - t$ è di Eisenstein rispetto a P

UFD (lemma di Gauss, Eisenstein)

$\rightarrow x^p - t = f(x)$ irriducibile in $\mathbb{F}_p[t][x]$ e quindi anche in $\mathbb{F}_p(t)[x]$ per il L. di Gauss

$\rightarrow$ Ovvero f è IRRIDUCIBILE e NON SEPARABILE

$$(\exists \alpha \in \bar{\mathbb{F}_p}: f(\alpha) = 0 \rightarrow \alpha^p = t \rightarrow f(x) = x^p - \alpha^p = (x - \alpha)^p)$$

Cor: $\forall \alpha \in \bar{K} \exists r$ tale che α^{p^r} è separabile su K . (dove $p = \text{char } K$)

Dim: $\alpha \rightarrow \mu_\alpha(x)$ irriducibile $\Rightarrow \exists r: \mu_\alpha(x) = g(x^{p^r})$ con g separabile

$$\Rightarrow 0 = \mu_\alpha(\alpha) = g(\alpha^{p^r}) \rightarrow \alpha^{p^r} \text{ è separabile}$$

il mio polinomio divide g che non ha radici multiple $\rightarrow$ rimuovo il polinomio n ha

Def: L/K algebrica di finito grado di separabilità di L/K e

$$[L:K]_s := \# \text{Hom}_K(L, \bar{K}) = \# \{ \sigma: L \rightarrow \bar{K} \mid \sigma|_K = \text{id} \}$$

• La definizione non dipende dalla scelta di $\bar{K}$, cioè $\Omega \cong \bar{K}$ allora

$$\text{Hom}_K \{L, \bar{K}\} \xrightarrow[\sigma \circ \varphi]{\sim} \text{Hom}_K(L, \Omega)$$

$$|\text{Hom}_K(L, \bar{K})| = |\{ \varphi: L \rightarrow \bar{K} \mid \varphi|_K = \text{id} \}|$$

Prop 1: $L = K(\alpha)$ algebrica: valgono i seguenti fatti

$$\textcircled{1} [K(\alpha):K]_s = \# \text{ radici distinte di } p_\alpha \text{ in } \bar{K}$$

$$\textcircled{2} \alpha \text{ e separabile} \Leftrightarrow [K(\alpha):K]_s = [K(\alpha):K]$$

$$\textcircled{3} \text{ Se } \text{char } K = p \text{ e } p^r \text{ e la molteplicità di } \alpha \text{ in } p_\alpha \text{ allora}$$

$$[K(\alpha):K] = p^r [K(\alpha):K]_s$$

Dim: $\textcircled{1} [K(\alpha):K]_s = \# \{ \varphi: K(\alpha) \rightarrow \bar{K} \mid \varphi(K) = \text{id} \}$
 $\xrightarrow[\text{into}]{\text{giù}}$ $= \# \text{ radici distinte di } p_\alpha \text{ in } \bar{K}$

$$\textcircled{2} [K(\alpha):K] = \deg(p_\alpha) \quad \alpha \text{ sep} \Leftrightarrow \deg p_\alpha = [K(\alpha):K]_s$$

$$[K(\alpha):K]_s = \# \text{ radici distinte di } p_\alpha \text{ in } \bar{K}$$

$$\textcircled{3} p_\alpha(x) = \prod_{i=1}^d (x - \alpha_i)^{p^r} \text{ con } \alpha_i = \alpha. \text{ Allora } [K(\alpha):K] = p^r d$$

dove $d = \# \text{ radici distinte di } p_\alpha \text{ in } \bar{K} = [K(\alpha):K]_s$.

Prop 2: $K \subset L \subset M \Rightarrow [M:K]_s = [M:L]_s [L:K]_s$

Dim:

$$\begin{pmatrix} M \\ L \\ K \end{pmatrix} \begin{array}{l} \{ \tau_j \}_{j \in J} \quad \tau_j: M \rightarrow \bar{K} : \tau_j|_L = \text{id} \\ \{ \sigma_i \}_{i \in I} \quad \sigma_i: L \rightarrow \bar{K} : \sigma_i|_K = \text{id} \end{array}$$

$\uparrow$
estendendo alle chiusure algebriche

Dico che $\text{Hom}_K(M, \bar{K})$ e $\{ \tilde{\sigma}_i \circ \tau_j \mid i \in I, j \in J \}$

$$\textcircled{1} \tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_{i'} \circ \tau_{j'} \Leftrightarrow i = i' \text{ e } j = j' \text{ (sono tutti distinti)}$$

restringo ad $L \rightarrow \tau_j|_L = \tau_{j'}|_L = \text{id} : (\tilde{\sigma}_i \circ \tau_j)|_L = \tilde{\sigma}_i|_L = \sigma_i$
 $(\tilde{\sigma}_{i'} \circ \tau_{j'})|_L = \tilde{\sigma}_{i'}|_L = \sigma_{i'} \rightarrow i = i'$

$$\textcircled{2} \tilde{\sigma}_i \circ \tau_j: M \rightarrow \bar{K} \text{ e } (\tilde{\sigma}_i \circ \tau_j)|_K = \text{id}, \text{ quindi } \exists \text{ ok}$$

$$\textcircled{3} \text{ Sia } \varphi: M \rightarrow \bar{K} : \varphi|_K = \text{id} \text{ allora } \varphi|_L \in \text{Hom}_K(L, \bar{K})$$

quindi $\varphi|_L = \sigma_i \Rightarrow \tilde{\sigma}_i^{-1} \circ \varphi: M \rightarrow \bar{K} \text{ e } (\tilde{\sigma}_i^{-1} \circ \varphi)|_L = \text{id}$
 $\Rightarrow (\tilde{\sigma}_i^{-1} \circ \varphi) = \tau_j \Rightarrow \varphi = \tilde{\sigma}_i \circ \tau_j$

Prop 3: L/K finita: se $\text{char } K = 0 \Rightarrow [L:K] = [L:K]_s$

• se $\text{char } K = p \rightarrow \exists r: [L:K] = [L:K]_s \cdot p^r$

Dim: $L = K(\alpha_1, \dots, \alpha_n)$ e uso l'induzione.

$F = K(\alpha_1, \dots, \alpha_{n-1})$ e $L = F(\alpha_n)$, allora

$$\begin{aligned} [L:K] &= [F(\alpha_n):K] = [F(\alpha_n):F][F:K] \\ &= p^r [F(\alpha_n):F]_s p^r [F:K]_s \\ &= p^r [F(\alpha_n):K]_s = p^r [L:K]_s \end{aligned}$$

Prop 4: L/K finita: sono equivalenti

- ① L/K è separabile
- ② L è generato su K da elementi separabili
- ③ $[L:K] = [L:K]_s$

Dim: $1 \Rightarrow 2$, ok
 $2 \Rightarrow 3$, $L = K(\alpha_1, \dots, \alpha_n)$ per induzione su n (P.B. per (2) prop 1)

P.I: $F = K(\alpha_1, \dots, \alpha_{n-1})$ e $L = F(\alpha_n) \rightarrow [L:K] = [F(\alpha_n):F][F:K]$
 $= [F(\alpha_n):F]_s [F:K]_s$
 $= [L:K]_s$

$3 \Rightarrow 1$, scelgo $\alpha \in L: [K(\alpha):K] = p^r [K(\alpha):K]_s$
 quindi α è separabile se e solo se $r = 0$.

Ma $[L:K] = [L:K(\alpha)][K(\alpha):K]$
 $= [L:K(\alpha)] p^r [K(\alpha):K]_s \geq p^r [L:K]_s$

e poiché $[L:K] = [L:K]_s \rightarrow r = 0$.

Prop 5: L/K algebraica. Sono fatti equivalenti:

- ① L/K separabile
- ② L è generata su K da elementi separabili

In questo caso $[L:K] = [L:K]_s$

esempio: $K = \mathbb{F}_p(t)$ e $L = \overline{\mathbb{F}_p(t)}$ vale L/K non separabile
 ma $[L:K] = +\infty$
 $[L:K]_s = +\infty$

Infatti $\mathbb{F}_p(t) \subset \overline{\mathbb{F}_p(t)} \subset \overline{\mathbb{F}_p(t)}$
 (non sep.)
 (sep e infinita)

Dim: $1 \Rightarrow 2$, ok
 $2 \Rightarrow 1$, $\alpha \in L = K(S) \Rightarrow \alpha = \sum_{i=1}^n k_i S_i$ con $S_i \in K(S_1, \dots, S_n)$ che è
 separabile $\leftarrow$ finita e separata da elementi separabili (Prop 4)

Voglio dimostrare che $[L:K] = [L:K]_s$

- $[L:K] < +\infty$ ok
- $[L:K] = +\infty$, voglio mostrare che $[L:K]_s = +\infty$

So che $\forall F \text{ t.c. } K \subset F \subset L, F \text{ separabile in } K$.
 Se $[F:K] < +\infty \Rightarrow [F:K] = [F:K]_s$.

Lemma: se $\forall F$ con $K \subset F \subset L, [F:K] \leq n_0 \Rightarrow [L:K] < +\infty$

Dim: $L = \bigcup_{\substack{F \subset L \\ [F:K] \text{ finito}}} F = \bigcup_{\alpha \in L} K(\alpha)$ allora suo $\bar{n} = \max_{\substack{F \subset L \\ [F:K] \text{ fin.}}} [F:K]$
 $\alpha \in L$ scrittura in pol. irriducibile

$\rightarrow F_0 \subseteq L$: se $\exists \alpha \in L \setminus F_0$,
 avrei che $[F_0(\alpha):K] > \bar{n}$ assurdo

$\Rightarrow F_0 = L \rightarrow L$ è finita

Quindi se $[L:K] = +\infty$ allora le sue sottoestensioni non possono avere grado uniformemente limitato:

$\forall n \exists F_n: K \subset F_n \subset L$ e $[F_n:K] > n$ e $[F_n:K]_s = [F_n:K]$
 $\Rightarrow [L:K]_s > [F_n:K]_s > n \quad \forall n \rightarrow [L:K]_s = +\infty$

* PROPRIETA' DELLE ESTENSIONI SEPARABILI

03/14

① TORRI:

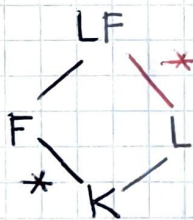


$\Leftrightarrow$
 $(\Rightarrow)$ Se L/K finita: $[L:K]_s = [L:F]_s [F:K]_s$
 $= [L:F][F:K]$
 $= [L:K]$

Se L/K infinita: $\alpha \in L$
 allora α separabile in F per ipotesi pol. min. in F
 $\rightarrow F_0 = K(\text{cof. di } \alpha) \subseteq F \Rightarrow K \subseteq F_0 \subseteq F_0(\alpha) \subseteq F$

Quindi α separabile in F_0 , finita $\rightarrow \alpha$ sep in K

② SHIFT:

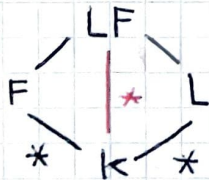


LF/L separabile: infatti

$LF = L(F)$ e $\forall \alpha \in F: \alpha$ sep in $K \subset L \Rightarrow \alpha$ sep in L ($K_\alpha(t)/K_\alpha(k)$)

Quindi LF generata da elementi separabili su L separabile in L .

③ COMPOSTO:



(1+2 $\rightarrow$ 3)

In generale L_i/K separabili $\Rightarrow L = \pi L_i = K(\bigcup_i L_i)$

è separabile perché separatamente generata.

Def: Si dice chiusura separabile di $L/K, K^s$, la più grande sottoestensione di L separabile su K

$$\equiv \bigcup_{F \subset L, L/K \text{ sep}} F$$

Oss: F/K separabile e $\tilde{F} = \prod_{\substack{\sigma: F \rightarrow K \\ \sigma|_K = \text{id}}} \sigma F$ e separabile su K [la chiusura normale e sep.]

• TEO [Elemento primitivo]

• L/K finita e separabile e semplice ($\exists \alpha \in \bar{K}: L = K(\alpha)$)

Dim: Caro 1: K finito $\Rightarrow L$ finito: $L = \langle \sigma \rangle \rightarrow L = K(\sigma)$

Caro 2: K infinito: $L = K(\alpha_1, \dots, \alpha_n)$ ma basta che dimostri il caso $n=2$ (+ induzione)

$$L = K(\alpha, \beta) \text{ e } [L:K] = n: \text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$$

$$\Rightarrow \text{sia } f(t) = \prod_{i \neq j} (\sigma_i(\alpha) + t \sigma_i(\beta) - \sigma_j(\alpha) - t \sigma_j(\beta))$$

$$1. f \neq 0: \sigma_i(\alpha) + t \sigma_i(\beta) = \sigma_j(\alpha) + t \sigma_j(\beta) \Leftrightarrow \begin{cases} \sigma_i(\alpha) = \sigma_j(\alpha) \\ \sigma_i(\beta) = \sigma_j(\beta) \end{cases}$$

ovvero se $\sigma_i = \sigma_j$

$$2. K \text{ infinito, } \exists t_{i,K}: f(t) \neq 0, \text{ ovvero per quanto } t$$

$$\pi(\sigma_i(\alpha) + t \sigma_i(\beta) - \sigma_j(\alpha) - t \sigma_j(\beta)) \neq 0$$

$$\pi(\sigma_i(\alpha + t\beta) - \sigma_j(\alpha + t\beta)) \neq 0$$

$$\text{Sia } \gamma := \alpha + t\beta \Rightarrow \sigma_i(\gamma) \neq \sigma_j(\gamma) \forall i \neq j$$

$$\rightarrow |\{\sigma_j(\gamma)\}| = n \text{ da cui } [K(\gamma):K] \geq n \rightarrow L = K(\gamma)$$

• TEO 1 L/K finita: L/K semplice $\Leftrightarrow |\{F | K \subset F \subset L\}| < +\infty$

• Dim: Caro 1: K finito: entrambe le condizioni sono banalmente vere

Caro 2: K infinito. Vediamo le due implicazioni

($\Rightarrow$) L/K semplice: $L = K(\alpha)$ e sia $K \subset F \subset L: L = F(\alpha)$.
Chiamiamo N_F il pol min di α su F : $N_F | N_K$

$$\{F | K \subset F \subset L\} \xrightarrow[N_F]{F} \{p(x) | N_F\}$$

e INIETTIVA. In fatti: dato N_F , sia $F_0 = K(\text{cef di } N_F)$ allora:

$$F_0 \subseteq F \subseteq F_0(\alpha) = F(\alpha) = L$$

$$\text{ma } N_{F_0} | N_F \text{ (} N_F \in F_0[x] \text{)}, N_F | N_{F_0} \text{ (} F_0 \subseteq F \text{)} \rightarrow N_F = N_{F_0} \rightarrow F = F_0$$

$$\text{Se } N_F = N_{F'} \text{ allora } F' = F_0 = F$$

$$\rightarrow |\{F | K \subset F \subset L\}| \leq |\{p(x) | N_F\}| < +\infty \checkmark$$

($\Leftarrow$) Come prima, facciamo il caso $L = K(\alpha, \beta)$

$\forall t \in K: K(\alpha + t\beta) \subset L$ ma i sottocampi di L/K sono in numero finito, ovvero

$\exists s \neq t$ t.c. $K(\alpha + s\beta) = K(\alpha + t\beta)$ ma qui volendo comb. lineari: $\alpha, \beta \in K(\alpha + s\beta)$

$\rightarrow L = K(\alpha + s\beta)$ e' semplice

Oss: TEO 1 + Corrispondenza di Galois $\Rightarrow$ TEO El. primitivo

L/K finita e separabile $\Rightarrow \tilde{L}/K$ sep e normale, $|\text{Gal}(\tilde{L}/K)| < \infty$ e FINITA

Quindi $\tilde{L}/K$ ha un # finito di sotto-estensioni e a maggior ragione anche L/K ha solo un numero finito di sotto-estensioni.

$\Rightarrow L/K$ semplice.

es: (Estensione ^{finita} non semplice) $L = \mathbb{F}_p(x, y)$ e $K = \mathbb{F}_p(x^p, y^p)$

Considero $\phi: L \rightarrow \tilde{L}$ ($\phi(L) = K$)
 $\alpha \quad \alpha^p$

① $K \subsetneq K(x) \subsetneq K(x, y) = L$ e vale

- $\mu_x(K) \mid t^p - x^p = (t-x)^p \xrightarrow{x \notin K} \mu_x(K) = t^p - x^p$ e $[K(x):K] = p$
char=p $[K(x):K]_s = 1$

- $\mu_y(K(x)) \mid t^p - y^p$ e come su, $\mu_y(K(x)) = t^p - y^p$, $[L:K(x)] = p$
 $[L:K(x)]_s = 1$

$\Rightarrow [L:K] = p^2$ ma $[L:K]_s = 1$: L/K finita non separabile

② Vediamo L/K non semplice, facendo vedere che ogni $\alpha \in L$ ha grado $\leq p$ su K (e quindi $K(\alpha) \subsetneq L \forall \alpha \in L$)

Poiché $K = \phi(L): \forall \alpha \in L, \alpha^p \in K \rightarrow \mu_\alpha(K) \mid t^p - \alpha^p$
ovvero $\deg(\mu_\alpha(K)) \leq p$

$\Rightarrow$ Per il teorema precedente quindi esistono infinite estensioni diverse fra K e L , ed in particolare

$K(\alpha + g\beta)$ con $g \in K$ sono tutte distinte

es: L/K finita, $\text{char } K = p$: α separabile su $K \Leftrightarrow K(\alpha) = K(\alpha^p)$

($\Rightarrow$) $\mu_\alpha(K(\alpha^p)) \mid t^p - \alpha^p = (t-\alpha)^p$ e α sep su $K \Rightarrow \alpha$ sep su $K(\alpha^p)$
quindi $\mu_\alpha = t - \alpha$ e $\alpha \in K(\alpha^p)$

($\Leftarrow$) $\mu_\alpha(K) = g(t^{p^r})$ per qualche r . Se $r > 0$, allora:

$\mu_{\alpha^p}(K) \mid g(t^{p^{r-1}}) \Rightarrow [K(\alpha^p):K] < [K(\alpha):K]$ an.

quindi $r = 0$ e α sep su K

* ESTENSIONI PURAMENTE INSEPARABILI

Oss: K campo, $\alpha \in \bar{K}$. Sappiamo $\mu_\alpha(x) = g(x^{p^r})$ con g separabile
 Allora:

$$\begin{array}{c} K(\alpha) \\ | \text{ } p^r \\ K(\alpha^{p^r}) \\ | \text{ } \text{sep.} \\ K \end{array}$$

$$- [K(\alpha^{p^r}) : K] = [K(\alpha) : K]_s$$

$$- [K(\alpha) : K] = p^r [K(\alpha^{p^r}) : K]$$

Quindi (per l'uni) $K(\alpha^{p^r})$ è la massima sottoestensione separabile di $K(\alpha)/K$

Def: L/K il grado di inseparabilità di L/K è $[L:K]_i = \frac{[L:K]}{[L:K]_s}$

[Moltiplicatività sulle torri] $\Rightarrow K-F-L$ allora $[L:K]_i = [L:F]_i [F:K]_i$
 pu. alg e degs

Def: $f \in K[x]$ si dice puramente inseparabile se ha un'unica radice in $\bar{K}$

f irriducibile e pur. inseparabile: $\text{char } K = 0 \rightarrow f = x - \alpha$
 $\text{char } K = p \rightarrow f = x^{p^r} - c$

Def: $\alpha \in K$ si dice puramente inseparabile se μ_α è puramente inseparabile
 $- L/K$ si dice puramente inseparabile se $\forall \alpha \in L$ è pur. insep su K

Oss: L/K pur. inseparabile $\Rightarrow L/K$ normale

$\sigma \in \text{Hom}_K(L, \bar{L})$: $\sigma(\alpha) \in \{\text{radice di } \mu_\alpha \text{ in } \bar{L}\} \stackrel{(*)}{=} \{\alpha\} \rightarrow \sigma(\alpha) = \alpha$
 $\forall \alpha \in L$

$L = K(\alpha)$ pur. inseparabile $\rightarrow [K(\alpha) : K]_s = 1$

Prop: L/K algebraica. Sono fatti equivalenti: $\text{char } K = p$

- ① L/K puramente inseparabile
- ② $L = K(S)$ con S t.c. $\forall s \in S$ s è pur. inseparabile
- ③ $[L:K]_s = 1$
- ④ $\forall \alpha \in L \exists r \geq 0$ t.c. $\alpha^{p^r} \in K$

Dim: $1 \Rightarrow 2$ ovvio

$2 \Rightarrow 3$: $[L:K]_s = |\text{Hom}_K(L, \bar{L})|$ e pu. dip. da $\sigma: L \rightarrow \bar{L}$: $\sigma|_K = \text{id}$
 baste definire $\sigma(s) \forall s \in S$ ($L = K(S)$)

Ma $\sigma(s) \stackrel{(*)}{=} s \forall s \in S$ poiché s pur. insep $\rightarrow \sigma = \text{id} \rightarrow [L:K]_s = 1$

$3 \Rightarrow 4$: $\alpha \in L$: $\mu_\alpha = g(x^{p^r})$ e vale $K \subseteq K(\alpha^{p^r}) \subseteq K(\alpha) \subseteq L$
 $[K(\alpha^{p^r}) : K] = [K(\alpha^{p^r}) : K]_s \leq [L:K]_s = 1 \xrightarrow{p^r} \alpha^{p^r} \in K$

$4 \Rightarrow 1$: $\alpha \in L$: $\mu_\alpha(x) \mid t^{p^r} - \alpha^{p^r}$ che è un polinomio pur. inseparabile $\rightarrow$ anche μ_α lo è
 (in campo)

In char = 0?

* PROPRIETA' DELLE ESTENSIONI PROPIAMENTE INSEPARABILI

① TORRI



Vale il $\Leftrightarrow$, infatti

$$[L:K]_s = [L:F]_s [F:I]_s [I:K]_s$$

② SHIFT



$$LF = F(L) \text{ e } \forall \alpha \in L$$

$$\mu_\alpha(F) \mid \mu_\alpha(L) \text{ pm. insp.}$$

③ COMPOSTO (1+2)



ef: L/K algebrica, $K^s = \{\alpha \in L : \alpha \text{ sep su } K\}$ chiusura sep di L/K 03/19

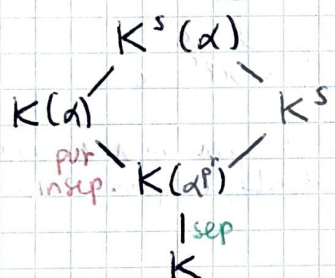
Teo: L/K algebrica $\Rightarrow$

- K^s/K separabile
- L/K^s pm. inseparabile
- e K^s è univocamente det. da queste proprietà

$$\text{Inoltre } [L:K]_s = [K^s:K], [L:K]_i = [L:K^s]$$

e se L/K è normale $\Rightarrow K^s/K$ è normale

Dim: Vediamo L/K^s pm. inseparabile. Sia $\alpha \in L$, vale dove $\mu_\alpha = g(x)^{e^r}$



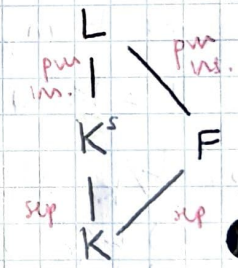
- α^{p^r} sep su K (il suo pol. min è $g(x)$), $\in K^s$
- SHIFT $\Rightarrow K^s(\alpha)/K^s$ pm. insp.

ovvero α è pm. inseparabile su $K^s \forall \alpha \in L$
 $\Rightarrow L/K^s$ pm. inseparabile

- Mostriamo che K^s è unico con tali proprietà

$$F/K \text{ sep} \Rightarrow F \subset K^s \quad K \subset F \subset K^s \subset L$$

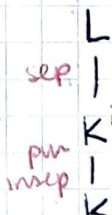
Dimmoli K^s/F è pm. inseparabile (bmi) $\rightarrow K^s = F$
 K^s/F è separabile (bmi)



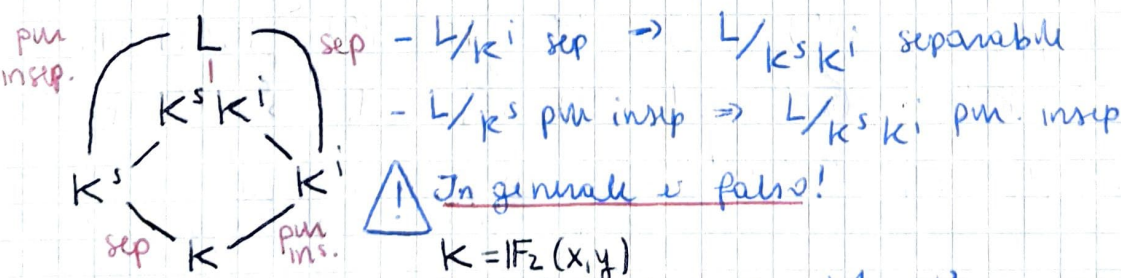
- $\alpha \in K^s$ e μ_α si fattorizza completamente in $L \Rightarrow$ ogni radice di μ_α è sep su K (bmi)
 $\Rightarrow K^s$ è cds di μ_α

Oss: L/K alg: potremmo voler costruire K^i tale che

- K^i/K pm. inseparabile
- L/K^i separabile



Ma allora pm. bmi vale:



! In generale è falso!

$$K = \mathbb{F}_2(x, y)$$

$$L = K(\alpha) \text{ dove } \mu_\alpha = t^4 + xt^2 + y \text{ ind.}$$

$\rightarrow$ si può vedere K^s/K normale, K^i/K normale ma L/K NON normale ($\neq K^s K^i$)

Teo: L/K normale $\Rightarrow \exists!$ sottoestensione K' di L/K t.c. $K \leq K' \leq L$ ^{pur. insep.} _{sep.}

Dim: $\text{Hom}_K(L, \bar{K}) = \text{Hom}_K(L, L) = \text{Aut}_K(L)$ (normalità)

● Sia allora $K' = \text{Fix}(\text{Aut}_K(L)) = \{ \alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in \text{Aut}_K(L) \}$

- è un campo

- $[K':K]_s = |\text{Hom}_K(K', \bar{K})| = |\text{Hom}_K(K', L)| = 1$ ^{def}
 poiché $\sigma: K' \rightarrow L$ si estende a $\tilde{\sigma} \in \text{Aut}_K(L)$ e $\tilde{\sigma}|_{K'} = \text{id} = \sigma$

(Inoltre è la massima sottoest. di L/K pur. inseparabile su K
 $\rightarrow$ ogni estensione di questo tipo è fissa da $\text{Aut}_K(L)$)

Mostriamo che L/K' è separabile: sia $\alpha \in L$, $f(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$

dove $\text{Orb}_{\text{Aut}_K(L)}(\alpha) = \{ \sigma_1(\alpha), \dots, \sigma_n(\alpha) \}$

- $\tau \in \text{Aut}_K(L) : \tau f = f \rightarrow f \in K[x] \rightarrow f \in K'[x]$

- f separabile e $\mu_\alpha(K') \mid f \Rightarrow \alpha$ separabile su K'

● Come prima si dimostra l'unicità di K' .

ex(5): $K = \mathbb{F}_2(x, y)$, $L = K(\alpha)$ e α radice di $\mu_\alpha(x) = t^4 + xt^2 + y = g(t^2)$

1. μ_α irriducibile (Eisenstein rispetto a $P = (x, y)$)

2. $[L:K]_i = 2$ e quindi $[L:K]_s = 2$

Per dimostrare che K' non esiste, basta far vedere che L/K ^{NON} NORMALE

Ora $g(z) = z^2 + xt + y = (z - \alpha)(z - \beta) = (z - \alpha^2)(z - \beta^2)$
 e quindi $\mu_\alpha = (z - \alpha)^2(z - \beta)^2$ (siamo in char 2)

Quindi L/K non normale $\Leftrightarrow \beta \notin L$: $\alpha^2 \beta^2 = y$
 $(\alpha + \beta)^2 = \alpha^2 + \beta^2 = x$

$\rightarrow \alpha\beta = \sqrt{y}$
 $\alpha + \beta = \sqrt{x}$

Se $\beta \in L \rightarrow \sqrt{x}, \sqrt{y} \in L \Rightarrow K(\sqrt{x}, \sqrt{y}) \subseteq L$ ma

$[K(\sqrt{x}, \sqrt{y}):K]_i = [K(\sqrt{x}, \sqrt{y}):K(\sqrt{x})]_i [K(\sqrt{x}):K]_i = 2 \cdot 2 = 4 > 2$
 an.

es: K campo, $\text{char } K = p$, allora $\phi: K \rightarrow K$ $\begin{smallmatrix} a \\ a^p \end{smallmatrix}$ suriettivo $\Leftrightarrow K$ perfetto

sol: $(\Rightarrow) \alpha \in \bar{K} : \mu_\alpha(x) = g(x^{p^r})$ con g separabile, inoltre ϕ suriettivo

$\mu_\alpha(x) = g(x^{p^r}) = (h(x))^{p^r}$ per qualche $h \rightarrow r=0$ per irriducibilità di μ_α

$(\Leftarrow)$ Sia $b \in K$, cerco β t.c. $\beta^p = b$ e $\beta \in K$

so che $\exists \beta \in \bar{K}$ t.c. β è radice di $x^p - b \Rightarrow \beta$ alg su K
 $\mu_\beta(x) = (x - \beta)^p = x^p - b$

Poiché K è perfetto $\rightarrow \mu_\beta$ è separabile
 ovvero $\mu_\beta = x - \beta \in K[x] \rightarrow \beta \in K$.

es: choi $K = \mathbb{F}_p$. $K^{p^{-n}} = \{a \in \bar{K} : a^{p^n} \in K\} \Rightarrow K \subseteq K^{p^{-1}} \subseteq \dots \subseteq K^{p^{-n}} \subseteq \dots$
 Sia allora $K^{p^{-\infty}} = \bigcup_{n \in \mathbb{N}} K^{p^{-n}}$

1. $K^{p^{-\infty}}$ è perfetto
2. K perfetto $\Leftrightarrow K^{p^{-\infty}} = K$ e $[K^{p^{-\infty}} : K] = \begin{cases} 1 & K \text{ perfetto} \\ \infty & \text{altrimenti} \end{cases}$

Sol: Osserviamo $K^{p^{-n}} = \text{Cds } \{x^{p^n} - a \mid a \in K\}$

1. $K^{p^{-\infty}}$ perfetto $\Leftrightarrow \phi$ Frobenius è suriettivo. Sia $a \in K^{p^{-\infty}}$, cerco $b \in K^{p^{-\infty}}$ tale che $b^p = a$.
 $a \in K^{p^{-\infty}} = \bigcup_n K^{p^{-n}} \rightarrow a \in K^{p^{-r}} : a = x^{p^r} \in K$

Cerco una soluzione di $x^p - a$ in $K^{p^{-\infty}}$ ma $(x^p - a)^{p^r} = x^{p^{r+1}} - a^{p^r} \in K[x]$
 $\Rightarrow$ In $K^{p^{r+1}}$ trovo tutte le radici di $x^{p^{r+1}} - a$ ($\rightarrow$ e quindi in $K^{p^{-\infty}}$)

2. $(\Leftarrow)$ ovvio
 $(\Rightarrow)$ K perfetto $\Rightarrow \phi$ Frobenius suriettivo $\rightarrow x^p - a$ si fattorizza in K ovvero $K^{p^{-1}} = K$
 ed iterando: $K^{p^{-n}} = K \forall n \rightarrow K = K^{p^{-\infty}}$

Inoltre, se K non è perfetto, sicuramente il Frobenius non è suriettivo.
 Ma allora $\exists a \in K$ t.c. $x^p - a$ è irriducibile: sia $\alpha_r \in \bar{K}$

Allora $\alpha_r \in K^{p^{-r}}$ e voglio $[K^{p^{-r}} : K] \geq [K(\alpha_r) : K] \stackrel{(\cdot)}{=} p^r$

Infatti $\mu_{\alpha_r} \mid (x - \alpha_r)^{p^r} = x^{p^r} - a \rightarrow \mu_{\alpha_r} = (x - \alpha_r)^{p^m} = x^{p^m} - \alpha_r^{p^m}$

Ma $r = \min \{k : \alpha_r^{p^k} \in K\}$ (se $\alpha_r^{p^m} \in K, m < k$: allora p^{r-m} -esimo di α_r , $\alpha_r^{p^m}$)

es: K campo, $L = K(\alpha, \beta)$ con α sep su $K \rightarrow L/K$ semplice

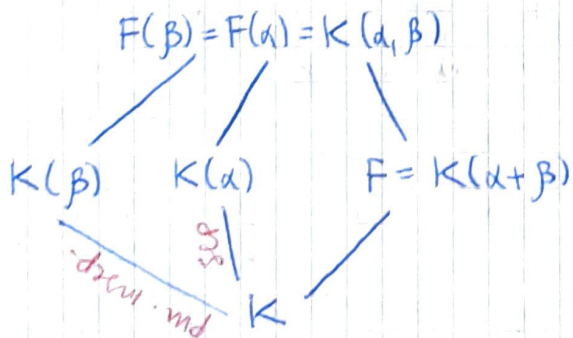
Sol: Il caso intervincente è $|K| = +\infty$. Sia $n = [L : K]_s = [K^s : K]$
 Guardiamo

$$F(x) = \prod_{i < j} (\sigma_i(\alpha) + t \sigma_i(\beta) - \sigma_j(\alpha) - t \sigma_j(\beta))$$

- $F \neq 0$
- $\exists t \in K \setminus 0 : K(t) \neq 0 \rightarrow [K(\alpha + t\beta) : K]_s = n \rightarrow K(\alpha + t\beta) \supseteq K^s \supseteq K(\alpha)$

$\Rightarrow \alpha \in K(\alpha + t\beta)$ e quindi anche $\beta \rightarrow K(\alpha, \beta) = K(\alpha + t\beta)$

es: L/K con $\alpha \in L$ sep su $K, \beta \in L$ pm insp su $K \Rightarrow K(\alpha\beta) = K(\alpha + \beta) = K(\alpha, \beta)$



Per shift:

$K(\alpha, \beta)/F$ è sia sep che pm insp

$\Rightarrow F = K(\alpha, \beta)$

Def: L/K si dice di Galois se $\bar{L}/\bar{K}$ è normale e separabile

$$\text{SEP} \Leftrightarrow \# \text{Hom}_K(L, \bar{K}) = [L:K]$$

$$\text{NORMALE} \Leftrightarrow \text{Hom}_K(L, \bar{K}) = \text{Aut}_K(L) =: \text{Gal}(L/K)$$

Prop 1: L/K normale, $K \subset E \subset L$, allora:

$$\textcircled{1} E/E \text{ è normale e } \text{Aut}_E(L) < \text{Aut}_K(L)$$

$$\textcircled{2} \text{ Se } E/K \text{ è normale } \Rightarrow \text{res}: \text{Aut}_K(L) \xrightarrow{\sigma} \text{Aut}_K(E) \xrightarrow{\sigma|_E} \text{Aut}_K(E) \text{ è surgettiva}$$

Dim (2): $\sigma \in \text{Aut}_K(L)$: $\sigma|_E: E \rightarrow L$ ma $\sigma|_E(E) = E$ (E/K norm)
 $\sigma|_E(K) = \sigma|_K = \text{id}$

Quindi res è ben definita.

Dimostro che $\forall T \in \text{Aut}_K(E), \exists \sigma \in \text{Aut}_K(L): \sigma|_E = T$

Infatti data T posso estenderla a $\sigma \in \text{Aut}_K(L)$

Prop 2: L campo, $G < \text{Aut}(L)$. Sia $K = L^G = \text{Fix}(G) = \{\alpha \in L \mid \sigma\alpha = \alpha \forall \sigma \in G\}$
Allora: C'è un campo.

$$\textcircled{1} |G| < +\infty \Rightarrow L/K \text{ di Galois finita con } \text{Gal}(L/K) = G$$

$$\textcircled{2} G \text{ infinito ma } L/K \text{ algebrica } \Rightarrow L/K \text{ di Galois e } G < \text{Galois}(L/K)$$

Dim: • Dico che se sono nelle ipotesi $\textcircled{1}$ o $\textcircled{2}$ allora L/K è separabile.

Sia $\alpha \in L$: $\text{orb}_G(\alpha) = \{\sigma_1(\alpha), \dots, \sigma_m(\alpha)\}$ è FINITA se G finito
o se L/K algebrica (G finita su K)

$$\Rightarrow f(x) = \prod_{i=1}^m (x - \sigma_i(\alpha)) \in K[x] \text{ perché } G \text{ fissa } f(x).$$

$\Rightarrow \mu_\alpha \mid f(x)$ che è separabile $\Rightarrow \mu_\alpha(x)$ è separabile

• L/K è normale: dico che $L = \text{Cd}_K \{ \mu_\alpha^{(\sigma)}(x) \mid \alpha \in L \}$

In fatti $\mu_\alpha(x) \mid f(x) = \prod (x - \sigma_i(\alpha))$ e $\sigma_i(\alpha) \in L$ perché $\sigma_i \in G < \text{Aut}(L)$.

$\Rightarrow L/K$ è di Galois

$$\text{Ovviamente } G < \text{Gal}(L/K) \rightarrow |G| \leq |\text{Gal}(L/K)| = [L:K]$$

Se $|G| < +\infty$ devo vedere che vale l'=".

$$\text{Dimostro che se } |G| = n \Rightarrow [L:K] \leq n.$$

$$\text{Per quanto so, } \deg \mu_\alpha(x) \leq n \Rightarrow [K(\alpha):K] \leq n$$

Ora $\forall K \subset F \subset L$, con $[F:K]$ finita $\rightarrow L/K$ sep $\Rightarrow F/K$ finita e separabile $\rightarrow$ intero e semplice

$$\Rightarrow \forall K \subset F \subset L \text{ finita } [F:K] \leq n \xrightarrow{\text{galo}} [L:K] \leq n$$

Cor 2: L/K normale, $G = \text{Aut}_K(L)$. Allora:

① L/L^G di Galois e $G = \text{Gal}(L/L^G)$

② Se L/K separabile $\Rightarrow L^G = K$ (caso particolare di ①)

③ $K \subset L^G \subset L$ done $L^G = K^i$ (questo mto)
pm. insp. sep

Dim (1): L/K normale $\Rightarrow$ algebrica $\xrightarrow{\text{Prop 2}} \begin{cases} L/L^G \text{ di Galois} \\ G \leq \text{Gal}(L/L^G) \end{cases}$

$$G \leq \text{Gal}(L/L^G) = \text{Aut}_{L^G}(L) \leq \text{Aut}_K(L) = G \rightarrow G = \text{Gal}(L/L^G)$$

es: [Prop 2 con L/L^G non algebrica]

03/28

$L = \mathbb{Q}(x)$ e $\phi \in P/A = \frac{P(x+k)}{q(x+k)}$, $\phi \in \text{Aut}(L)$.

Allora $L^{\langle \phi \rangle} = \left\{ \frac{p(x)}{q(x)} \mid \frac{p(x+k)}{q(x+k)} = \frac{p(x)}{q(x)} \quad \forall k \in \mathbb{Z} \right\} = \mathbb{Q} \Rightarrow L/L^{\langle \phi \rangle} \simeq \mathbb{Q}(x)/\mathbb{Q}$
e mto mto g??

TEOREMA [Corrispondenza di Galois - 1^a parte]

L/K di Galois e $G = \text{Gal}(L/K)$. Allora:

$$\begin{array}{ccc} \{H \mid H \leq G\} & \xrightleftharpoons[\psi]{\phi} & \{F \mid K \subseteq F \subseteq L\} \\ H & & F \end{array}$$

e valgono:

$$\psi(F) = \text{Gal}(L/F)$$

F

ben def
su tutti

① $\phi \circ \psi = \text{id}$ ($\Rightarrow \psi$ iniettiva, ϕ surgettiva)

② $|G| < +\infty \Rightarrow$ allora anche $\psi \circ \phi = \text{id}$ (ψ, ϕ biunivoche)

③ F/K normale $\Leftrightarrow \text{Gal}(L/F) \triangleleft G$

In tal caso $\text{Gal}(F/K) \simeq G/\text{Gal}(L/F)$

Dim: ① $(\phi \circ \psi)(F) = \phi(\text{Gal}(L/F)) = L^{\text{Gal}(L/F)} = F$ Cor 2 con $K=F$

② $|G| < +\infty$: $(\psi \circ \phi)(H) = \psi(L^H) = \text{Gal}(L/L^H) = H$ Prop 2

③ F/K normale $\Rightarrow \forall \sigma \in G = \text{Gal}(L/K)$: $\sigma F = F$ (*)

ogni immersione di $F \hookrightarrow \bar{K}$
 $\uparrow$ estende a $L \hookrightarrow \bar{K} \Rightarrow L \rightarrow L$
 perché L/K normale

$\text{Gal}(L/F) \triangleleft G \Leftrightarrow \forall \sigma \in \text{Gal}(L/K)$, $\sigma \text{Gal}(L/F) \sigma^{-1} = \text{Gal}(L/F)$

(*) $\sigma F = F \leftarrow \psi \text{ iniett. } \psi(\sigma F) = \text{Gal}(L/\sigma F) = \text{Gal}(L/F) = \psi(F)$

In tal caso considero $\text{Gal}(L/K) \xrightarrow{\text{res}} \text{Gal}(F/K)$ che ha nucleo

$$\{\sigma : L \rightarrow L \mid \sigma|_F = \text{id}\} = \text{Gal}(L/F) \rightarrow \text{Gal}(F/K) \simeq \frac{\text{Gal}(L/K)}{\text{Gal}(L/F)}$$

ex [$\forall \phi \neq \text{id}$ se l'estensione è infinita] $\mathbb{F}_p$ e $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$

- $[\overline{\mathbb{F}_p} : \mathbb{F}_p] = +\infty$ e poiché $\mathbb{F}_p$ è perfetto $\rightarrow \overline{\mathbb{F}_p}$ è algebrica + separabile

- $\phi : \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ fissa $\mathbb{F}_p \Rightarrow H = \langle \phi \rangle < \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = G$

Osserviamo che: $\overline{\mathbb{F}_p}^H = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^p = \alpha\} = \mathbb{F}_p = \overline{\mathbb{F}_p}^G$

Mostriamo però che $H \neq G \rightarrow$ quindi la con. non è biunivoca

$H \cong \mathbb{Z}$ quindi tutti i stir di H hanno indice finito.

D'altra parte $F = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{2^n}}$ e t.c. $\mathbb{F}_p \subsetneq F \subsetneq \overline{\mathbb{F}_p}$

e via corrispondente di Galois F corrisponde a un stir di G di indice ∞
 $\rightarrow G$ ha stir di indice $\infty \Rightarrow H \subsetneq G$.

Cor: L/K finita e separabile $\Rightarrow$ ha un # finito di estensioni intermedie ($\rightarrow$ è semplice)

Dim: $\tilde{L} = \bigcup \sigma L$ chiusura normale di L finita $\rightarrow \text{Gal}(\tilde{L}/K)$ finito
 Ovvero esistono un # finito di sottocampi di $\tilde{L}$ (e a maggior ragione di L)

Cor2: L/K di Galois, H e $H' < \text{Gal}(L/K)$, allora

1. $LH \subset LH' \Leftrightarrow H' \subset H$
2. $LH LH' = L^{H \cap H'}$
3. $LH \cap LH' = L^{<H, H'>}$

Dim: 1. ovvio
 2. $H \cap H' \subset H, H' \Rightarrow LH LH' \supset L^{H \cap H'}$

Inoltre $\text{Gal}(L/LH) \cap \text{Gal}(L/LH') \supseteq H \cap H' \supset \text{Gal}(L/L^{H \cap H'})$

Da cui (con Φ) $LH LH' \subset L^{H \cap H'}$

3. uguale

Teo: L/K di Gal finita e $K \subset F \subset L \Rightarrow LF/F$ di Galois
 Inoltre $\text{Gal}(LF/F) \simeq \text{Gal}(L/L \cap F)$ ed inoltre $[LF:F] \mid [L:K]$

Dim: LF/F di Galois per shift di SEP + NORM di L/K

Allora res: $\text{Gal}(LF/F) \rightarrow \text{Gal}(L/L \cap F)$ è ben def.

è iniettiva $\Rightarrow H = \text{res}(\text{Gal}(LF/F)) < \text{Gal}(L/L \cap F)$

Ora $L^H \supset L \cap F$, d'altra parte $\alpha \in L^H: \sigma \alpha = \alpha \forall \sigma \in \text{Gal}(LF/F): \alpha \in F, \alpha \in L \cap F$

TEO2: $L/K, F/K$ di Galois finite $\rightarrow$ - LF/K di Galois
 - res: $\text{Gal}(LF/K) \rightarrow \text{Gal}(L/K) \times \text{Gal}(F/K)$ e' iniettivo
 - $K = L \cap F \Leftrightarrow$ res surgettiva

Dim: E' unico da dimostrare e la terza.

• $L \cap F = K$, allora sia $\sigma \in \text{Gal}(L/K)$, $\tau \in \text{Gal}(F/K)$
 $\Rightarrow$ Estendo σ, τ a LF trovando $\tilde{\sigma}, \tilde{\tau}$ dove $\tilde{\sigma}|_F = \text{id}$
 $\tilde{\tau}|_L = \text{id}$
 $\rightarrow \text{res}(\tilde{\sigma} \circ \tilde{\tau}) = (\sigma, \tau) \checkmark$

• res surg + iniettivo $\rightarrow |\text{Gal}(LF/K)| = |\text{Gal}(L/K)| |\text{Gal}(F/K)|$
 ovvero $[LF:K] = [L:K][F:K]$, ovvero

$$\underbrace{[L:F]}_{\leq} \underbrace{[F:L \cap F]}_{\leq} = \underbrace{[L:L \cap F]}_{\leq} \underbrace{[F:K]}_{\leq} \rightarrow [F:L \cap F] = [F:K]$$

ovvero $L \cap F = K$

Prop 1: $\deg f = n$ e $\alpha_1, \dots, \alpha_n$ radici di f , allora, $L = \text{Cds di } f$

03/29

$$\varphi: \text{Gal}(L/K) \xrightarrow{\sigma} S(\alpha_1, \dots, \alpha_n) \text{ e' omo iniettivo}$$

$\sigma|_{\alpha_i}, i=1, \dots, n$

Dim: Ben definito poich' $\sigma(\alpha_i) \in \{\text{radici di } p(\alpha_i)/f\} \subset \{\alpha_1, \dots, \alpha_n\}$
 Inoltre e' iniettivo e' ovvio: $L = K(\alpha_1, \dots, \alpha_n)$ e se $\sigma(\alpha_i) = \alpha_i \forall i \rightarrow \sigma = \text{id}$
 $\sigma|_K = \text{id}$

Prop 2: f irriducibile ($L = \text{Cds}(f)$) $\Leftrightarrow \text{Gal}(L/K) \ni \{\alpha_1, \dots, \alpha_n\}$ e' transitiva

Dim: f irriducibile: $f = k \cdot p$ con p pol. minimo di ogni radice di f
 Ma allora $\forall \alpha: f(\alpha) = 0$ tale che $\{\text{conjugati di } \alpha\} = \{\alpha_1, \dots, \alpha_n\}$
 e quindi $\forall i \neq j$ trova $\sigma(\alpha_i) = \alpha_j$.

In generale invece dato un qualsiasi polinomio f ,
 $\text{Gal}(L/K)$ permuta transitivamente le radici dei fattori irriducibili

Cor: $[L:K] = n$, L/K di Galois. Allora $\text{Gal}(L/K) < S_n$

Dim: (Teo. el. primitivo) $L = K(\alpha) = \text{Cds di } p_\alpha$ con $\deg p_\alpha = n$ + Prop 1

Def: Un'estensione di Galois n dice abeliana, se il suo gruppo di Galois e' abeliano, ciclico, se il suo gruppo di Galois e' ciclico.

* PROPRIETA' DI ESTENSIONI (*) ABELIANE / (*) CICLICHE

① TORRI



$$\begin{aligned} \text{Gal}(L/F) &\trianglelefteq \text{Gal}(L/K) \\ \text{Gal}(F/K) &\cong \frac{\text{Gal}(L/K)}{\text{Gal}(L/F)} \end{aligned}$$



$$\begin{aligned} K &= \mathbb{Q} \\ F &= \mathbb{Q}(\sqrt{2}) \\ L &= \mathbb{Q}(\sqrt[4]{2}) \end{aligned}$$

② SHIFT



$$\text{Gal}(L/F) \leq \text{Gal}(L/K)$$

③ COMPOSTO



$$\text{Gal}(L/F) \hookrightarrow \text{Gal}(L/K) \times \text{Gal}(F/K)$$

* CAMPI CICLOTOMICI

- ζ_n radice di $x^n - 1$ primitiva e ha $\phi_n = \mu_{\zeta_n} \Rightarrow x^n - 1 = \prod_{d|n} \phi_d$
- $U_n = \{ \alpha \in \overline{\mathbb{Q}} : \alpha^n = 1 \} \subset \overline{\mathbb{Q}}^*$ e $|U_n| = |\{ \text{radici di } x^n - 1 \}| = n \rightarrow U_n = \langle \zeta_n \rangle$
- $\mathbb{Q}(\zeta_n) = \mathbb{Q}(U_n) = \text{cds di } x^n - 1 \text{ e di Galois su } \mathbb{Q}$
- e $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, $\text{Gal}\left(\frac{\mathbb{Q}(\zeta_n)}{\mathbb{Q}}\right) \cong \mathbb{Z}/n\mathbb{Z}^*$

$$\text{Oss: } \mathbb{Q}(\zeta_m) \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$$

$$\subseteq: n/[m,n] \rightarrow \zeta_{[m,n]}^{m/d} \text{ ha ordine } \frac{[m,n]}{m/d} = \frac{mn}{d} \cdot \left(\frac{m}{d}\right)^{-1} = n \cdot \zeta_n \in \mathbb{Q}(\zeta_{[m,n]})$$

$$\supseteq: \text{ se } \frac{m}{a} + \frac{n}{b} = 1 \rightarrow \zeta_n^a \zeta_m^b = \zeta_{[m,n]}^{b \cdot \frac{m}{a} + a \cdot \frac{n}{b}} = \zeta_{[m,n]}$$

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d) \quad d = (m,n)$$

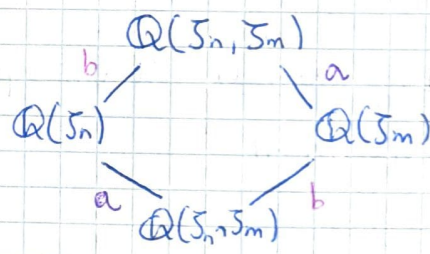
$$[\mathbb{Q}(\zeta_{[m,n]}): \mathbb{Q}] = \phi([m,n]) = \frac{\phi(m)\phi(n)}{\phi(d)}$$

$$\rightarrow \phi([m,n]) = abk \phi(d)$$

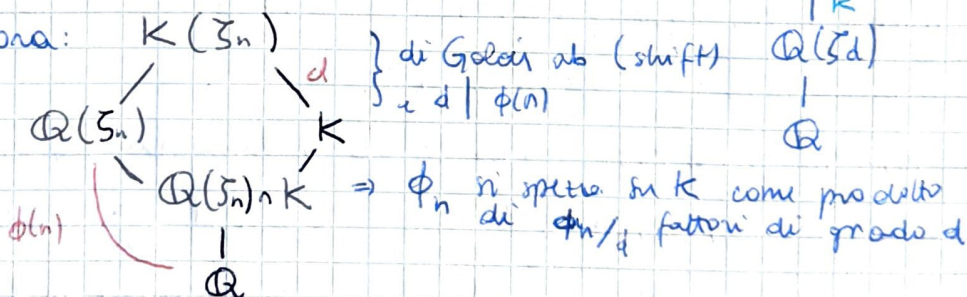
$$\phi(m) = b^2 k \phi(d)$$

$$\phi(n) = a^2 k \phi(d)$$

$$\rightarrow k^2 = k \rightarrow k = 1$$



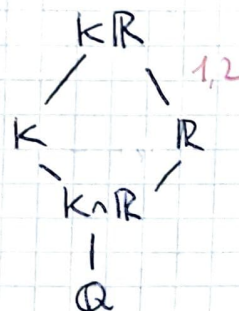
Oss: $\mathbb{Q} \subset K$ allora:



• Sottocampo reale di $K/\mathbb{Q}$ (di Galois)

$$K\mathbb{R}/\mathbb{R} \text{ abeliana} \Rightarrow K\mathbb{R} = \begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases}$$

$$\rightarrow [K : K \cap \mathbb{R}] = [K\mathbb{R} : \mathbb{R}] = \begin{cases} 1 & \mathbb{R} \subset K \\ 2 & \mathbb{R} \not\subset K \end{cases}$$



$K = \mathbb{Q}(\zeta_n) \rightarrow n > 2$ tale $[K : K \cap \mathbb{R}] = 2$, si verifica che

$\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{R}$ *simmetrie del coniugio*
 inoltre $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$

$(x - (\zeta_n + \zeta_n^{-1}) + x^{-1})x \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
 e si annulla in ζ_n

$\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Es: $a \in \mathbb{N}^+$, $K = \mathbb{Q}(\sqrt{-a})$. Mostrare che K non si può immergere in una estensione ciclica di $\mathbb{Q}$ di grado multiplo di 4

Sol: • Le estensioni cicliche di grado n hanno un unico stirpe di ordine a di n e questo è ciclico.
 $\rightarrow [K : \mathbb{Q}] = 2 \rightarrow$ basta per vedere che $\nexists E/\mathbb{Q} : [E : \mathbb{Q}] = 4$ ciclica, $K \subseteq E$

Supp. per assurdo che esiste, allora $E \xrightarrow{2} K \xrightarrow{2} \mathbb{Q}$

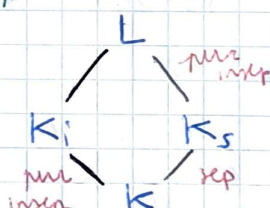
• $K \not\subseteq \mathbb{R}, K \subseteq E$: E non è reale $\rightarrow$ la sua sotto-estensione reale K' è t.c. $\{ [E : K'] = 2, K' \subseteq \mathbb{R} \}$

Ma quindi K, K' corrispondono a $H, H' \leq \mathbb{Z}/4\mathbb{Z}$ sottogruppi di ordine 2
 $\rightarrow$ ASS

Es 8: L/K algebrico: - K perfetto $\Rightarrow L$ perfetto
 - L perfetto, L/K finita $\Rightarrow K$ perfetto

Sol: 1) $\alpha \in \bar{K}, \beta = \sqrt[p]{\alpha} \in L$: $L(\beta) \xrightarrow{\text{alg}} L \xrightarrow{\text{alg}} K$
 $\beta \text{ sep in } K \xrightarrow{(F)} \beta \text{ sep in } L$

Es 10: L/K normale, $\text{char } K = p$. $L = K_i K_s$
 (già unito)



Es 11: L/K algebrico t.c. ogni $f \in K[x]$ irriducibile ha almeno una radice in L
 $\rightarrow L$ è una chiusura algebrica di K

Sol: (da 10): $\bar{K} = K_i K_s$, voglio $\bar{K} \subseteq L \rightarrow$ dimostro $K_i \subseteq L, K_s \subseteq L$.

• $\forall \alpha \in K_i, p_\alpha(K)(x) = x^{p^r} - \beta = (x - \alpha)^{p^r} \xrightarrow{\text{ip.}} \alpha \in L : K_i \subseteq L$

• $\forall \alpha \in K_s, p_\alpha(K)(x) \in K[x]$ ed ha una radice in L

Sia allora $F = K(\alpha_1, \dots, \alpha_n)$ CdS di $p_\alpha(K)$ in K
 $\rightarrow$ tro elemento primitivo $F = K(\beta)$ e p_β si spezza completamente su $F \rightarrow$ ogni radice di p_β genera F

(1p) L contiene una radice di $p_\beta \rightarrow F \subseteq L$
 $\Rightarrow \alpha \in L : K_s \subseteq L$

* TOPOLOGIA DI KRULL SU $\text{Gal}(L/k)$

04/02

L/k di Galois, $\mathcal{L} = \{L_i \mid L_i/k \text{ finita e di Galois}, L_i \subseteq L\} = \{L_i \mid i \in I\}$

$\Rightarrow L = \bigcup_{i \in I} L_i$ e $\forall i$ ho res: $\text{Gal}(L/k) \rightarrow \text{Gal}(L_i/k)$
 $\alpha \text{ alg.}$
 $\deg p_{\alpha, L_i} < \infty$

$\Rightarrow$ Sia $p: \text{Gal}(L/k) \rightarrow \prod_{i \in I} \text{Gal}(L_i/k) : p(\sigma) = (\sigma|_{L_i})_{i \in I}$

• omomorfismo

• iniettivo: $\sigma_i = \text{id}_{L_i} \forall i \Rightarrow \alpha \in L \rightarrow K(\alpha) = L_i \Rightarrow \sigma(\alpha) = \sigma_i(\alpha) = \alpha$

Dimostriamo $p(\text{Gal}(L/k)) = \{(\sigma_i)_{i \in I} \text{ coerenti}\}$ $L_i \subseteq L_j \Rightarrow \sigma_j|_{L_i} = \sigma_i$

$\subseteq$: ovvio

$\supseteq$: $\alpha \in L \Rightarrow \alpha \in L_i$ e sia $\sigma(\alpha) = \sigma_i(\alpha)$: ben definito per lo coerente (σ_i)
 $(\alpha \in L_i \cap L_j : \sigma_i(\alpha) = \sigma_j|_{L_i}(\alpha) = \sigma_k(\alpha) \checkmark)$
 Allora $p(\sigma) = (\sigma_i)_{i \in I}$

Vogliamo definire una topologia su $\text{Gal}(L/k)$

① Su $\text{Gal}(L_i/k)$ [finita] $\leftarrow$ topologia discreta

② $\prod_{i \in I} \text{Gal}(L_i/k)$ topologia prodotto

③ $p(\text{Gal}(L/k)) \subseteq \prod_{i \in I} \text{Gal}(L_i/k)$ topologia di sottospazio

④ $\text{Gal}(L/k)$ topologia indotta da p

Oss: In ② una base di aperti e $\{\prod_{i \in I} V_i\}_{i \in I}$ con $V_i = \begin{cases} \text{Gal}(L_i/k) \\ \{\sigma_i\} \end{cases}$
 $\{p^{-1}(\prod_{i \in I} V_i)\} = \{\sigma \text{Gal}(L/L_i) : \sigma|_{L_i} = \sigma_i\}$ pre-base

In realtà e' una BASE DELLA TOPOLOGIA INDOTTA DA p

$$\sigma \text{Gal}(L/L_i) \cap \tau \text{Gal}(L/L_j) = \left(\bigcup_{k=1}^n \sigma^{(k)} \text{Gal}(L/L_i) \right) \cap \left(\bigcup_{h=1}^m \tau^{(h)} \text{Gal}(L/L_j) \right) \\ = \bigcup_{k \in A} \sigma^{(k)} \text{Gal}(L/L_j)$$

$\Rightarrow (\text{Gal}(L/k), \langle \{\sigma \text{Gal}(L/L_i)\}_{\sigma_i} \rangle)$ e' un gruppo topologico

Basta mostrare che $m: (\sigma, \tau) \mapsto \sigma \circ \tau$ e $i: \sigma \mapsto \sigma^{-1}$ sono continue

$$i^{-1}(\sigma \text{Gal}(L/L_j)) = \text{Gal}(L/L_j) \sigma^{-1} = \sigma^{-1} \text{Gal}(L/L_j) \quad \text{poich\'e } \text{Gal}(L/L_i) \triangleleft \text{Gal}(L/k) \text{ in quanto } L_i/k \text{ \textbf{e} Galois}$$

$$m^{-1}(\sigma \text{Gal}(L/L_j)) = \{(\eta, \tau) : \eta \circ \tau \in \sigma \text{Gal}(L/L_j)\} \\ = \{(\eta, \tau) : (\eta \circ \tau)|_{L_j} = \sigma|_{L_j}\} = \bigcup_{\eta} \eta \text{Gal}(L/L_j) \times (\eta^{-1} \circ \sigma) \text{Gal}(L/L_j)$$

$\Rightarrow$ Inoltre la base e' fatta di clami laterali di stirg normali di indice finito

Oss: $\{\text{Gal}(L/L_i)\}$ interni di 1 (potremmo definire la top. con)

Oss: In un gruppo topologico i stgr aperti sono anche chiusi

$$H < G \Rightarrow G = \bigcup_{g \in G} gH \text{ ma quindi } G \setminus H = \bigcup_{g \neq e} gH \text{ aperto perche' } U \text{ di aperti}$$

TEO: $\text{Gal}(L/K)$ con la topologia di Krull e T_2 , cmpt e tot. sconnesso

Dim: - $\text{Gal}(L_i/K)$ con la topologia discreta e T_2 , cmpt, tot. sconnesso

- Hamdorff: $\sigma, \tau \in \text{Gal}(L/K), \sigma \neq \tau \Rightarrow \exists \alpha: \sigma(\alpha) \neq \tau(\alpha), \alpha \in L_i$
 $\rightarrow \sigma|_{L_i} \neq \tau|_{L_i} \rightarrow \sigma \in \sigma \text{Gal}(L/L_i), \tau \in \tau \text{Gal}(L/L_i)$
 $\text{e } \sigma \text{Gal}(L/L_i) \cap \tau \text{Gal}(L/L_i) = \emptyset$ ($\sigma \tau^{-1}(\alpha) = \sigma(\alpha) \neq \tau(\alpha) = \tau(\alpha)$ $\forall \tau, \sigma \in \text{Gal}(L/L_i)$)

- cmpt: basta mostrare $\rho(\text{Gal}(L/K))$ chiuso in $\pi \text{Gal}(L/K)$

Ora $\rho(\text{Gal}(L/K)) = \{ \text{succ. coerenti} \}$ e sia (σ_i) non coerente

$\rightarrow \exists L_n \subset L_i$ t.c. $\sigma_i|_{L_n} \neq \sigma_n \Rightarrow \sigma_j \in \pi V_j^{h_i}$ con $V_j^{h_i} = \{ \sigma \mid \sigma|_{L_n} = \sigma_n \}$
 e $\pi V_j^{h_i}$ e' un intorno di (σ_i) che non contiene successioni coerenti.

- tot. sconnesso: le componenti connesse del prodotto sono i pt

TEO [Corrispondenza di Galois - II parte]

$$\{ H < G : H = \overline{H} \} \longleftrightarrow \{ F \mid K \subseteq F \subseteq L \}$$

$$\begin{array}{ccc} \text{Gal}(L/F) & \xleftarrow{\psi} & F \\ H & \xrightarrow{\phi} & L^H \end{array}$$

e valgono: • $\psi = \phi^{-1}$

qui // who • F/K normale $\Rightarrow \text{Gal}(L/F) \triangleleft \text{Gal}(L/K)$
 e in tal caso $\text{Gal}(F/K) \cong \text{Gal}(L/K) / \text{Gal}(L/F)$

Dim: • ψ ben definita, cioe' $\forall F, \psi(F) = \text{Gal}(L/F)$ chiuso in G

$$\text{In fatti } \text{Gal}(L/F) = \bigcap_{\substack{K \subset F_i \subset F \\ F_i/K \text{ fin Gal}}} \text{Gal}(L/F_i) \quad \text{stgr aperti (e quindi chiusi)} \text{ in } G$$

dove: $\subseteq$: ch
 $\supseteq$: $\sigma \in \text{Gal}(L/F_i) \forall i \rightarrow F = \bigcup F_i$ e $\alpha \in F \rightarrow \exists i: \alpha \in F_i$
 $\Rightarrow \sigma(\alpha) = \alpha \rightarrow \sigma|_F = \text{id} \checkmark$

• ψ iniettiva visto

• ψ surgettiva: $H < G$ t.c. $H = \overline{H} \Rightarrow \text{Gal}(L/L^H) = H$

- Gal 1: $H = \text{Gal}(L/L^H)$

- Mostriamo che $\boxed{\sigma \in \text{Gal}(L/L^H) \Rightarrow \sigma \in \overline{H}}$: sia $L^H \subset F \subset L$ $\swarrow$ fin + Gal

allora $\sigma \text{Gal}(L/F) \cap H \neq \emptyset$. Infatti:

vale $LH \subseteq F \subseteq L \xrightarrow{H} LH \subseteq F^H \subseteq LH \Rightarrow LH = F^H$, ovvero

res: $H \rightarrow \text{Gal}(F/LH) \Rightarrow$ poiché F/LH finita, $F^{\text{res } H} = L^H$
 $\Rightarrow \text{res } H = \text{Gal}(F/L^H)$
 Gal

Così $\forall \gamma \in \text{Gal}(F/LH) \exists \gamma \in H: \gamma|_F = \gamma$ e per $\gamma = \sigma|_F$ troviamo $\gamma \in H \cap \sigma \in \text{Gal}(L/F)$.

$\Rightarrow$ Già visto $\phi \circ \gamma = \text{id} + \gamma$ surgettiva $\Rightarrow \gamma$ big e $\gamma = \phi^{-1}$

ex: $\mathbb{F}_p: \langle \phi \rangle \subset \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) = G$ e abbiamo visto che

$$\mathbb{F}_p = \mathbb{F}_p G = \mathbb{F}_p \langle \phi \rangle \rightarrow G = \langle \phi \rangle$$

Prop: $\frac{I}{F}$ stirg aperti di $\text{Gal}(L/K)$ corrispondono alle sottoestensioni di indice finito.

Dim: F/K finita + normale $\Rightarrow \text{Gal}(L/F)$ aperto

$\parallel G$ compatto $\Rightarrow H < G$ aperto ha indice finito, perché $G = \bigcup \sigma H$

Scelto $H < G$ aperto $\Rightarrow F = L^H$ e valgo $[F:K] = [G:H] < +\infty$

$L \supseteq F = L^H \supseteq K$ se F/K di Galois $\rightarrow$ ovvio

$$\text{Altrimenti } [F:K] = \# \text{Hom}_K(F, \bar{K}) = |\{ \sigma: F \rightarrow \bar{K}: \sigma|_F = \text{id} \}| = |\{ \sigma: H \rightarrow \bar{K} \}| = [G:H]$$

es: $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}$ con p_i primi distinti: $\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$

es: $\text{Gal}(\mathbb{Q}(\sqrt{m} | m \in \mathbb{Z}^+)/\mathbb{Q})$?

* GRUPPI PROFINITI

01/04

Def: Un gruppo profinito è un gruppo topologico, di Hausdorff, compatto e con una base di intorni di 1 fatta da stirg normali.

$\rightarrow \text{Gal}(L/K)$ è un gruppo profinito

Def: $(I, \leq)$ insieme parzialmente ordinato n' dice diretto se $\forall i, j \in I \exists k$ t.c. $i \leq k, j \leq k$

Def: Un sistema proiettivo di gruppi (famiglia di oggetti) è

$\{G_i, f_{ij}\}_{i, j \in I}$ dove:

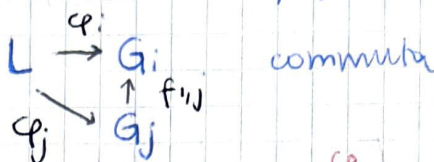
- I insieme diretto
- $f_{ij}: G_j \rightarrow G_i$ omomorfismi t.c.
- $f_{ii} = \text{id}$
- $f_{ik} = f_{ij} f_{jk}$

$$\begin{array}{ccc} G_j & \xrightarrow{f_{jk}} & G_k \\ f_{ji} \uparrow & & \nearrow f_{ki} \\ G_i & & \end{array}$$

Def: Si dice limite proiettivo (inverso) del sistema proiettivo $\{G_i, f_{ij}\}_{i, j \in I}$ e n' indica con $\varprojlim G_i = G$ l'elemento universale del sistema proiettivo nella categoria

Dato $\{G_i, f_{i,j}\}_{i,j}$, si dice elemento universale $G = \{G_i, f_i\}_{i \in I}$ t.c.

- $f_i: G \rightarrow G_i$ omo continui ed inoltre $\forall i \in I, \varphi_i$ t.c.
- $\forall i \leq j: f_{i,j} \circ f_j = f_i$



$\Rightarrow \exists \varphi: L \rightarrow G$ tale che $\begin{array}{ccc} L & \xrightarrow{\varphi} & G \\ & \searrow \varphi_i & \downarrow f_i \\ & & G_i \end{array} \quad \text{commuta}$

Oss: l'elemento universale κ esiste e' unico

Nel nostro caso $G = \varprojlim G_i = \{(\sigma_i)_{i \in I} \in \prod G_i \mid \forall i \leq j, f_{i,j}(\sigma_j) = \sigma_i\}$
(soddisfa le ipotesi + uniche)

Prop: $\{G_i\}$ gruppi topologici T2 e $f_{i,j}$ omo continui
allora $\varprojlim G_i$ chiuso in $\prod G_i$

(vedi - del 01/02)

Teo: • G profinito e $\{N_i\}$ sgr normali aperti $\Rightarrow [G: N_i] < +\infty$ (5.11)
Inoltre $\varprojlim G/N_i \cong G$ dove $i \leq j$ se $N_j \subset N_i$ e $\pi_{i,j}: G/N_j \rightarrow G/N_i$
 $\uparrow$ iso + omo

• $\{G_i, f_{i,j}\}$ sistema proiettivo di gruppi finiti (topologia discreta)
allora $G = \varprojlim G_i$ e profinito

(no dim)

ex: $\{\mathbb{Z}/p^n\mathbb{Z}, \pi_{n,m}\}_{n \leq m}$ allora: $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(\sigma_n)_{n \in \mathbb{N}} \mid \sigma_n \in \mathbb{Z}/p^n\mathbb{Z}, \pi_{n,m}(\sigma_m) = \sigma_n\}$

Ora $\pi_{n,m}(\sum_{i=0}^{m-1} a_i p^i) = \sum_{i=0}^{n-1} a_i p^i \Rightarrow (\sigma_n)$ e' univocamente det da $\{a_i\}_{i \in \mathbb{N}}$

$\Rightarrow \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{\sigma = \sum_{n \geq 0} a_n p^n \mid a_i \in \mathbb{Z}/p\mathbb{Z}\}$ ANELLO degli interi p-adi

ex: $\{\mathbb{Z}/m\mathbb{Z}, \pi_{n,m}\}_{n|m}$ sia $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z} = \{(\sigma_n)_{n \in \mathbb{N}} \text{ coerenti}\}$

① $\hat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p$ (isomorfismo + omeomorfismo)

Consideriamo $\varphi: \hat{\mathbb{Z}} \longrightarrow \prod \mathbb{Z}_p$ ben def e omo
 $(\sigma_n) \longmapsto \{(\sigma_{p^n})_{n \in \mathbb{N}}\}_p$

- φ iniettiva: $\varphi((\sigma_n)) = 0 \Rightarrow \sigma_{p^n} = 0 \forall p, n: m = p_1^{e_1} \dots p_k^{e_k}$
allora $\sigma_m \equiv \sigma_{p_1^{e_1}} \equiv 0 \pmod{p_1^{e_1}} \forall i \xrightarrow{\text{TCR}} \sigma_m \equiv 0 \pmod{m}: \sigma_m = 0 \forall$
- φ surgettiva: $\{(\sigma_{p^n})_{n \in \mathbb{N}}\}_p$ e' solo $\sigma_n \pmod{p^n}$ TCR.

Infine φ omo perche' intorno di (σ_n) vanno in intorno $\varphi((\sigma_n))$

② $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \{(\sigma_i) \in \prod \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \text{ coerenti}\} = \varprojlim \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$

(*) Faciamo vedere che $\{\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p), \text{res}_{n,m}\} \cong \{\mathbb{Z}/m\mathbb{Z}, \pi_{n,m}\}_{n|m}$

Se (*) vale, allora: $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$

(*) Basta osservare che $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\text{res}_{\text{nm}}} \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ commuta

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi_{nm}} & \mathbb{Z}/n\mathbb{Z} \\ \uparrow \phi & & \uparrow \phi \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi_{nm}} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

Oss: $\mathbb{F}_{p^{+\infty}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}}$ ovviamente $[\mathbb{F}_{p^{+\infty}} : \mathbb{F}_p] = +\infty$
e anche $[\mathbb{F}_p : \mathbb{F}_{p^{q^n}}] = +\infty$

04/109

$\Rightarrow L_q = \mathbb{F}_{p^{+\infty}}$ vale $\text{Gal}(L_q/\mathbb{F}_p) = \varprojlim \text{Gal}(\mathbb{F}_{p^{q^n}}/\mathbb{F}_p) \simeq \mathbb{Z}_q$

$\simeq \varprojlim \mathbb{Z}/q^n\mathbb{Z}$

Sia allora F un campo: $\mathbb{F}_p \subset F \subset L_q$ e sia $q^n = \sup \{ [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \mid \alpha \in F \}$
Dico che $F = \mathbb{F}_{p^{q^n}}$ (o L_q se $q^n = +\infty$)

$\subseteq$: se $n = +\infty$ ovvio,
 $n < +\infty$ allora $\forall x \in F : [\mathbb{F}_p(x) : \mathbb{F}_p] \mid q^n \rightarrow x \in \mathbb{F}_{p^{q^n}}$

$\supseteq$: se $n < +\infty$: $\exists \alpha \in F$ t.c. $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = q^n : \mathbb{F}_p(\alpha) = \mathbb{F}_{p^{q^n}} \subseteq F$

$n = +\infty$: $\forall n \exists x \in F$ t.c. $[\mathbb{F}_p(x) : \mathbb{F}_p] > q^n \rightarrow \mathbb{F}_{p^{q^n}} \subseteq F \quad \forall n \rightarrow L_q \subseteq F$

$\Rightarrow$ Le sottoestensioni di $L_q/\mathbb{F}_p$ sono tutte e sole gli $\mathbb{F}_{p^{q^n}}$

In termini di stir di $\mathbb{Z}_q$, questo significa che i stir chiusi sono solo i $\text{Gal}(L_q/\mathbb{F}_{p^{q^n}})$ al variare di $n \in \mathbb{N}$

Osserviamo che, detto ϕ il Frobenius di $L_q/\mathbb{F}_p$, si ha che ϕ^{q^n} fissa $\mathbb{F}_{p^{q^n}}$ e non $\mathbb{F}_{p^{q^{n+1}}}$

$\rightarrow \text{Gal}(L_q/\mathbb{F}_{p^{q^n}}) = \langle \phi^{q^n} \rangle \stackrel{(\ast)}{\cong} q^n \mathbb{Z}_q$

Cerchiamo ora le sottoestensioni di $\overline{\mathbb{F}_p}$. Sia $\mathbb{F}_p \subset F \subseteq \overline{\mathbb{F}_p}$

$\forall q$ guardiamo $F_q = F \cap L_q \Rightarrow F = \prod_{q \text{ primi}} F_q$ ($\geq$) ovvio

se $x \in F \Rightarrow [\mathbb{F}_p(x) : \mathbb{F}_p] = q_1^{\alpha_1} \cdots q_n^{\alpha_n} \Rightarrow x \in \mathbb{F}_{p^{q_1^{\alpha_1} \cdots q_n^{\alpha_n}}} \subseteq F_{q_1} \cdots F_{q_n}$
($y = x^{q_1^{\alpha_1} \cdots q_n^{\alpha_n}} \in \mathbb{F}_{p^{q_1^{\alpha_1}}} \cap F_{q_1} \subseteq F_{q_1}$)

Inoltre $F_q \subset L_q \rightarrow F_q \simeq \mathbb{F}_{p^{q^n}} \rightarrow F = \prod_{q \text{ primi}} \mathbb{F}_{p^{q^n}}$

Il stir chiuso di $\hat{\mathbb{Z}}$ che fissa F sarà $\text{Gal}(\overline{\mathbb{F}_p}/F) \simeq \prod_q q^n \mathbb{Z}_q$
 $\simeq \bigcap_q ((q^n \mathbb{Z}_q) \prod_{p \neq q} \mathbb{Z}_p)$

ex: $\mathbb{Q}(\sqrt{m} \mid m \in \mathbb{Z}) = K$ e $K = \mathbb{Q}(i, \sqrt{p} \mid p \text{ primi})$

e rappresentiamo un tale $G = \varprojlim \text{Gal}(F/\mathbb{Q})$ $F/\mathbb{Q}$ Gal + finita

In realtà mi basta una sottofamiglia filtrante, tipo $K_n = \mathbb{Q}(i, \sqrt{p_1}, \dots, \sqrt{p_n}) \Rightarrow G = \varprojlim (\mathbb{Z}/2\mathbb{Z})^n \simeq \prod_1^\infty \mathbb{Z}/2\mathbb{Z}$

Def: Gruppo di Galois assoluto di K è $\text{Gal}(\overline{K}/K)$

Def: $K^{ab} = \prod_{K \subseteq F \atop ab} F \equiv \prod_{K \subseteq F \atop ab+fn} F$

(Teo Kronecker-Weber) Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in una estensione ciclotomica

$\rightarrow \mathbb{Q}^{ab} = \mathbb{Q}(\zeta_n | n \in \mathbb{N}) \Rightarrow \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

da cui $\text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^*$ dove $n|m$ e mappa di restrizione
 $\stackrel{\text{verifica}}{=} \hat{\mathbb{Z}}^*$ $\mathbb{Q}(\zeta_1, \dots, \zeta_n) \subseteq \mathbb{Q}(\zeta_m)$

04/16

* TEORIA INVERSA DI GALOIS

Prop1: Tutti i gruppi abeliani finiti si realizzano in $\mathbb{Q}$

[Teo (Dummit)] $\forall a, n \in \mathbb{N}: (a, n) = 1 \Rightarrow \exists a + kn | n \in \mathbb{N}$ contiene a primi

Dim: $G \cong \prod_{i=1}^k \mathbb{Z}/n_i \mathbb{Z}$ si realizza in $\mathbb{Q}$ per induzione in k

P.B: $G \cong \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists p \equiv 1 \pmod{n} \Rightarrow \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$, $n | p-1$
 $\rightarrow \exists H < \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) : G \cong \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})/H$ e sia $F = \mathbb{Q}^H$
 $\rightarrow \text{Gal}(F/\mathbb{Q}) \cong G$

P.I: $\{p_i\}_{i=1}^k : p_i \equiv 1 \pmod{n_i} \rightarrow F_i/\mathbb{Q}$ t.c. $\text{Gal}(F_i/\mathbb{Q}) \cong \mathbb{Z}/n_i \mathbb{Z}$

Ora $\mathbb{Q}(\zeta_{p_1+1}, \zeta_{p_2}) \cap \mathbb{Q}(\zeta_{p_1+1}) = \mathbb{Q}$ se p_i distinti
 $\rightarrow \prod F_i \cap F_{k+1} = \mathbb{Q}$ e per il lemma $F = \prod_{i=1}^k F_i \rightarrow \text{Gal}(F/\mathbb{Q}) \cong \prod \mathbb{Z}/n_i \mathbb{Z}$

Prop2: $\forall G$ gruppo finito $\exists L/K$ t.c. $G = \text{Gal}(L/K)$

Dim: - [Cayley] $G \hookrightarrow S_n$ con $n = |G|$

- Se trova (*) L/F t.c. $\text{Gal}(L/F) \cong S^n \stackrel{S^n \text{ finito}}{\Rightarrow} \text{Gal}(L/L^G) \cong G$

(*) $t_1, \dots, t_n$ indeterminati in K campo $\rightarrow L = K(t_1, \dots, t_n)$ allora
 $S_n \hookrightarrow \text{Aut}_K(L)$ in modo che $\sigma \in S_n \Rightarrow \sigma(t_i) = t_{\sigma(i)}$
 $\sigma|_K = \text{id}$

Ma quindi L/L^{S_n} ha gruppo di Galois S_n

Oss: L^{S_n} è il campo delle funzioni simmetriche

Siano $s_1 = \sum_{i=1}^n t_i$, $s_2 = \sum_{i < j} t_i t_j$, ..., $s_n = \prod_{i=1}^n t_i : s_i \in L^{S_n} \forall i$

Dimostriamo che $L^{S_n} = \langle s_1, \dots, s_n \rangle_K = K(s_1, \dots, s_n)$

$p(x) = \prod_{i=1}^n (x - t_i) = \sum_{i=0}^n (-1)^i s_i x^{n-i} \in K(s_1, \dots, s_n)[x]$

$\rightarrow K(t_1, \dots, t_n) = \text{CdS di } p \text{ su } K(s_1, \dots, s_n)$
 ovvero $[L : K(s_1, \dots, s_n)] = d \leq n!$

$\begin{matrix} L \\ | \\ n! \\ S_n \\ | \\ L \\ || \\ K(s_1, \dots, s_n) \end{matrix}$ (en)

Prop3: ① $K(S_1, \dots, S_n) = K(T_1, \dots, T_n)^{S_n} = F$
 con L/F di Galois e $\text{Gal}(L/F) \cong S_n$

② $S_1, \dots, S_n$ sono algebricamente indipendenti

Def: $A \subset L$ si dice **ALGEBRICAMENTE INDIPENDENTE** su K se gli elementi di A non soddisfano nessun polinomio non nullo a coeff. in K .

U: $A = \{a\}$ A alg indep in $K \iff a$ è trascendente su K

es: $A = \{t, t+1\}$ anche se sono entrambi trascendenti annullano $x - y + 1$.

Dim: Siano $S_1, \dots, S_n$ indeterminate e considero:

$f(x) = x^n - S_1 x^{n-1} + S_2 x^{n-2} - \dots + (-1)^n S_n \in K(S_1, \dots, S_n)[x]$
 e siano $t_1, \dots, t_n$ le radici di $f(x)$ in una fissata chiusura algebrica di $K(S_1, \dots, S_n)$.

Considero l'omomorfismo $K(T_1, \dots, T_n) \xrightarrow[\tau_i]{\phi} K(t_1, \dots, t_n)$

$\Rightarrow$ restringo ϕ a $\phi_i: K(S_1, \dots, S_n) \rightarrow K(t_1, \dots, t_n)$
 $\downarrow \quad \quad \quad \downarrow$
 $S_i \quad \quad \quad t_i$

iso $\{ \rightarrow \cdot \text{Im}(\phi_i) = K(S_1, \dots, S_n) \}$
 $\cdot \phi_i$ è non nullo $\rightarrow$ (def in un campo) quindi **INIETTIVO**

Se $S_1, \dots, S_n$ fossero algebricamente dipendenti, allora lo sarebbero anche le S_i , ma questo non è possibile perché sono indeterminate distinte.

Voglio trovare S_n come gruppo di Galois su $\mathbb{Q}$

① TEO [irriducibilità di Hilbert] (no dim)

Sia $r \geq 1$ e sia $f(T_1, \dots, T_n, X_1, \dots, X_r) \in \mathbb{Q}[T_1, \dots, T_n, X_1, \dots, X_r]$
 irriducibile. Allora esistono infinite n -ple $(a_1, \dots, a_n) \in \mathbb{Q}^n$
 tali che

$f(a_1, \dots, a_n, X_1, \dots, X_r) \in \mathbb{Q}[X_1, \dots, X_r]$ è irriducibile

② TEO: $\forall n \geq 2$ il gruppo S_n si realizza in $\mathbb{Q}$

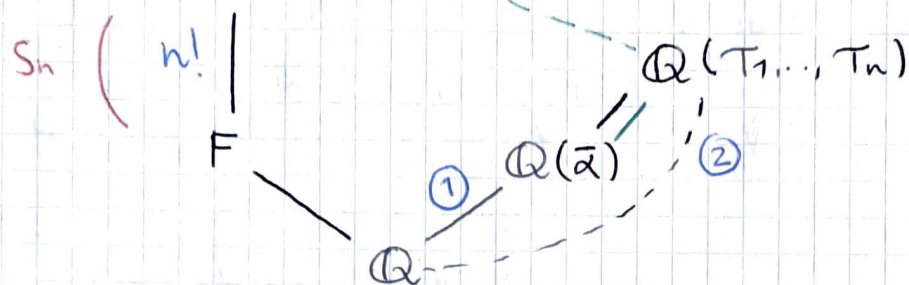
Dim: $L = \mathbb{Q}(T_1, \dots, T_n)$ e $F = \mathbb{Q}(S_1, \dots, S_n)$ e L/F ha $\text{Gal} \cong S_n$
 L/F finita e separabile $\rightarrow$ TEO del primitivo: $L = F(\alpha(T_i))$
 dove $\alpha(T_i) \in \mathbb{Q}[T_1, \dots, T_n]$

$\triangle$ Sia $P = P_\alpha(T_i) \in \mathbb{Q}[S_1, \dots, S_n][x] = F[x]$ e radici di $\{\alpha(T_i)\}$
 $\forall i=1, \dots, n$

$\rightarrow P \in \mathbb{Q}[S_1, \dots, S_n, x]$ con S_i alg. indipendenti
 $\deg_x P = n!$ e P irriducibile

$\rightarrow \exists (a_1, \dots, a_n) \in \mathbb{Q}^n$ t.c. $P(a_1, \dots, a_n, x) \in \mathbb{Q}[x]$ e irrid.

e dette $T_1, \dots, T_n$ radici di $f(x) = x^n - a_1 x^{n-1} + \dots + (-1)^n a_n$
 $\Rightarrow P(a_1, \dots, a_n, x)$ ha radici $\{\alpha_i(T_1, \dots, T_n)\}$ quindi $P(a_1, \dots, a_n, x)$
 ha grado $n!$ in x

$$F(\{T_i\}) = L = F(\alpha(\{T_i\}))$$


② $\mathbb{Q}(T_1, \dots, T_n)$ est Cds sur $\mathbb{Q}$ car $f(x) = x^n a_1 x^{n+1} + \dots + (-1)^n a_n$
 $\Rightarrow \mathbb{Q}(T_1, \dots, T_n)/\mathbb{Q}$ est de Galois sur $\mathbb{Q}$ car $\deg \leq n!$

inoltre $\text{Gal}(\mathbb{Q}(\bar{\alpha})/\mathbb{Q}) \hookrightarrow S_n$ e per cardinalità

$$\text{Gal}(\mathbb{Q}(\bar{\alpha})/\mathbb{Q}) \cong S_n$$

Δ Posso scegliere $\alpha = T_1 + 2T_2 + \dots + nT_n \rightarrow p(x) = \prod (x - \sigma(T_1 + 2T_2 + \dots + nT_n))$
 $\Rightarrow p \in F[x]$ ma anche a $\mathbb{Q}[S_1, \dots, S_n][x]$

* RESULTANTE E DISCRIMINANTE

- $f(x) = \sum_{i=1}^n a_i x^i$, $g(x) = \sum_{i=1}^m b_i x^i$: $(f, g) \neq 1 \Leftrightarrow \exists f_1, g_1 \in K[x]$ $\deg f_1 < n$
 $\deg g_1 < m$

and $(f, g) \neq 1 \Rightarrow$ eig. $\lambda(x)f(x) + \mu(x)g(x) = 0$ $f g_1 = g f_1$
 has solutions or not.

$$\Leftrightarrow \underbrace{\det(\text{Syl}(f, g))}_{R \text{ is } (f, g)} = 0$$

Oss. $\text{Ris}(f_{ij})$ è un polinomio omogeneo in $\mathbb{Z}[a_1, \dots, a_n, b_1, \dots, b_m]$

- $f(x) \in K[x]$ con $f(x) = a \prod_{i=1}^n (x - \alpha_i)$ allora definiamo

$$\text{disc}(f) = \Delta_f = a^{2(n-1)} \prod_{i < j} (\alpha_i - \alpha_j)^2$$

Oss. - Δ_f è indipendente dall'ordine delle radici di f (elevo al quadrato)
 - Il coef. serve a fare in modo che $\Delta_f \in \mathbb{Z}[\text{coef di } f]$

Prop 1: $Ris(f, f'') = (-1)^{\frac{n(n-1)}{2}} \text{adisc}(f)$

Bem: $f = a \prod_{j=1}^n (x - \alpha_j)$ e $f'(x) = a \sum_{j=1}^n \prod_{i \neq j} (x - \alpha_i)$

$$\text{Res}(f, f') = a^{n-1} \prod_{i=1}^n f'(\alpha_i) = a^{n-1} \prod_{i=1}^n a \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j) = \left(a^{2(n-1)} \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j)^2 \right) (-1)^{\frac{n(n-1)}{2}} a$$

Ex: $f = ax^2 + bx + c \rightarrow \Delta_f = \frac{\text{Ris}(f, f')}{(-1)^n a} = \frac{1}{-a} \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = b^2 - 4ac$
 $f = x^3 + ax + b \rightarrow \Delta_f = -4a^3 - 27b^2$

• Vale che: $\text{disc } f = \frac{\text{Ris}(f, f')}{(-1)^n a} \in \mathbb{Z}[\text{coef di } f]$ ed è divisibile per a (la prima colonna e tutte multiple di a) $\rightarrow \text{disc } f \in \mathbb{Z}[\text{coef } f]$

• $\text{disc } f = 0 \Leftrightarrow \text{Ris}(f, f') = 0 \Leftrightarrow (f, f') \neq 1 \Leftrightarrow f$ ha fattori multipli.

- $f \in K[x] \Rightarrow L = K(\alpha_1, \dots, \alpha_n)$ Cds di f : allora

$$\Delta_f = a^{2(n-1)} \prod_{i < j} (\alpha_i - \alpha_j)^2 \in K$$

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j) \in L \text{ ma in generale } \notin K : \delta^2 = \Delta_f \cdot a^{-(2n-2)} \in K$$

CASO: $\delta \in K$

Si agisce su $\{\alpha_1, \dots, \alpha_n\}$ e $\forall \sigma \in S_n: \sigma \Delta_f = \Delta_f$
 mentre $\sigma \delta = \pm \delta$
 (ad esempio $\tau = (12) \rightarrow \tau \delta = -\delta$)

Prop: $G = \text{Gal}(L/K) : G \subseteq A_n \Leftrightarrow \Delta_f \in K^{\wedge 2} \Leftrightarrow \delta \in K$

Dim: $\delta \in L \rightarrow \delta \in K = L^G \Leftrightarrow \forall \sigma \in G \sigma \delta = \delta \Leftrightarrow \sigma \in A_n$

es1: f irriducibile di grado 3 $\rightarrow G = \text{Gal}(f) = \begin{cases} S_3 \\ A_3 \end{cases}$
 $\wedge \text{Gal}(f) = A_3 \Leftrightarrow \Delta_f = \square$

es2: f irriducibile: $f(x) = x^4 + ax^2 + b \in K[x]$, $\text{char } K \neq 2$

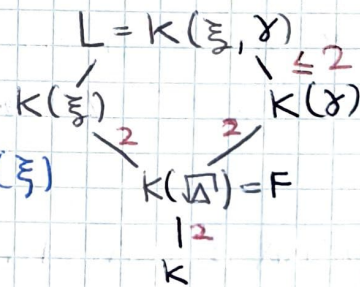
$G = \text{Gal}(f) < S_4 \Rightarrow$ sia $g(x) = x^2 - ax - b$, $\Delta_g = a^2 - 4b \notin K^{\wedge 2}$
 e $g(x) = (x - \alpha)(x - \beta)$ con $\alpha, \beta \in \bar{K}$

$\Rightarrow K(\alpha) = K(\beta) = K(\sqrt{\Delta_g})$ e sono $\pm \gamma = \sqrt{\alpha}$, $\pm \xi = \sqrt{\beta}$

$\Rightarrow f(x) = (x - \gamma)(x + \gamma)(x - \xi)(x + \xi)$, allora

$$\text{Anche } [L:K] = 4 \cdot [K(\xi, \gamma) : K(\xi)] =$$

$= 4 \Leftrightarrow K(\xi, \gamma) = K(\xi) \Leftrightarrow \gamma \in K(\xi) \Leftrightarrow K(\gamma) = K(\xi)$
 ma ora $K(\gamma) = F(\sqrt{\alpha}) = F(\sqrt{\beta}) = K(\xi)$
 estensioni quadratiche, quindi coincidono
 e solo se $\alpha\beta = b \in F^{\wedge 2}$ (*)



$= 8 \Leftrightarrow b \notin F^{\wedge 2} \rightarrow |G| = 8$ e $G < S_4 \rightarrow G \cong D_4$

(*) se $b \in F^{\wedge 2} \rightarrow |G| = 4$ e $G < S_4$ ha 2 con $G = \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2 & G \subseteq A_4 \\ \mathbb{Z}_4 & G \not\subseteq A_4 \end{cases}$

e per distinguere gli ultimi con basterà calcolare il discriminante di f e vedere se $\in K^{\wedge 2}$.

$\Delta_f = 16 \gamma^2 \xi^2 (\gamma^2 - \xi^2)^4 = 16 \alpha \beta (\alpha - \beta)^4 = 16 b (\Delta_g)^2$ e $b \in K(\sqrt{\Delta})^2$

$\Delta_f \in K^{\wedge 2} \Leftrightarrow b \in K^{\wedge 2} \rightarrow G \cong \begin{cases} \mathbb{Z}_{1/2}\mathbb{Z} \times \mathbb{Z}_{1/2}\mathbb{Z} & b \in K^{\wedge 2} \\ \mathbb{Z}_{1/4}\mathbb{Z} & b \notin K^{\wedge 2} \end{cases}$

*TEO D'INDIPENDENZA DEI CARATTERI DI ARTIN

G gruppo, K campo: un carattere di G in K è un omonorfismo

$$\chi : G \longrightarrow K^*$$

- Esiste sempre $\chi(g) \equiv 1$, carattere banale

$(\{\chi : G \rightarrow K^*\}, \cdot)$ $((\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g))$ è un gruppo

e $\{\chi : G \rightarrow K^*\} \subset \text{App}(G, K)$

Teo [indipendenza dei caratteri di Artin]

Caratteri distinti in G sono linearmente indipendenti

Dim: Siano $\chi_1, \dots, \chi_n$ t.c. $a_1\chi_1 + a_2\chi_2 + \dots + a_n\chi_n = 0$ (*)
è una relazione di dipendenza lineare di lunghezza minima

→ per minimalità $a_i \neq 0 \forall i$

$$\forall g \in G: \text{valutando (*) in } g \text{ trovo} \\ a_1\chi_1(g) + a_2\chi_2(g) + \dots + a_n\chi_n(g) = 0 \quad (1)$$

Inoltre χ_i distinti: $\exists h \in G: \chi_1(h) \neq \chi_2(h)$

$$\Rightarrow a_1\chi_1(gh) + a_2\chi_2(gh) + \dots + a_n\chi_n(gh) = 0 \text{ ovvero}$$

$$a_1\chi_1(h)\chi_1(g) + a_2\chi_2(h)\chi_2(g) + \dots + a_n\chi_n(h)\chi_n(g) = 0 \quad (2)$$

$$\stackrel{(1) \cdot \chi_1(h)}{\Rightarrow} a_1\chi_1(h)\chi_1(g) + a_2\chi_2(h)\chi_2(g) + \dots + a_n\chi_n(h)\chi_n(g) = 0 \quad (1')$$

$$\Rightarrow (2) - (1'): \underbrace{a_2(\chi_2(h) - \chi_1(h))}_{\alpha_2}\chi_2(g) + \dots + \underbrace{a_n(\chi_n(h) - \chi_1(h))}_{\alpha_n}\chi_n(g) = 0 \quad \forall g$$

→ $\alpha_2\chi_2(g) + \dots + \alpha_n\chi_n(g) = 0$ e per minimalità di (*)
dove valere

$$\alpha_i = 0 \quad \forall i \rightarrow \text{ma } i=2$$

$$\begin{cases} \chi_2(h) \neq \chi_1(h) \text{ per def} \\ a_2 \neq 0 \text{ per ip} \end{cases} \rightarrow \underline{\text{Ass.}}$$

* NORMA E TRACCIA

Def: L/K di grado finito, $\alpha \in L$: allora

$$\phi_\alpha : L \xrightarrow{x} L \quad \text{moltiplicazione per } \alpha$$

$$\phi_\alpha \text{ è } K\text{-lineare} \Rightarrow \text{Tr}_{L/K}(\alpha) = \text{tr } \phi_\alpha$$

$$N_{L/K}(\alpha) = \det \phi_\alpha$$

Oss: $\text{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in K \quad \forall \alpha$ purché $\phi_\alpha \in M_{n \times n}(K)$

ex: $z \in \mathbb{C}, N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2$ lineare norma di gruppo infatti $\phi_z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ $x+z = a+ib$ rispetto a $\{1, i\}$

Lemma 1: Sia $n = [L:K]$. Allora:

1) $a \in K \Rightarrow \text{Tr}_{L/K}(a) = na, N_{L/K}(a) = a^n$

2) $L = K(\alpha)$ e $p_\alpha(x) = x^n + C_1 x^{n-1} + \dots + C_n \rightarrow \text{Tr}_{L/K}(\alpha) = -C_1, N_{L/K}(\alpha) = (-1)^n C_n$

Dim: 1) $[\varphi_\alpha] = a \cdot \text{In}_{n \times n}$

2) p_α è POL. CARATTERISTICO di φ_α : $\begin{cases} p_\alpha(\varphi_\alpha)(x) = p_\alpha(x)(x) = 0 \\ \deg p_\alpha = n \end{cases}$

e p_α irreducibile $\rightarrow$ pol minimo di φ_α

p_α è anche pol caratteristico perché $\deg p_\alpha = n = \dim L/K$ ($L = K(\alpha)$)

Lemma 2: L/K finita, $\alpha \in L$ e $[L:K(\alpha)] = s$, allora:

$$\text{Tr}_{L/K}(\alpha) = s(\text{Tr}_{K(\alpha)/K}(\alpha)) \text{ e } N_{L/K}(\alpha) = (N_{K(\alpha)/K}(\alpha))^s$$

Dim: p_α = pol min di α su K = pol min di φ_α su K ($\uparrow$)

Quindi poiché p_α è irreducibile

$\deg p_\alpha(x) = \dim L/K = s \deg p_\alpha \rightarrow p_\alpha(x) = (p_\alpha(x))^s$

$$p_\alpha(x) = (x^n + C_1 x^{n-1} + \dots + C_n)^s = x^{sn} + sC_1 x^{sn-1} + \dots + C_n^s$$

Prop 1: L/K finita e $[L:K] = \underbrace{[L:K]}_q \cdot \underbrace{[K(\alpha):K]}_r$, sono inoltre

$$\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_r\}$$

Allora $\alpha \in L \rightarrow \text{Tr}_{L/K}(\alpha) = q \sum_{i=1}^r \sigma_i(\alpha), N_{L/K}(\alpha) = \left(\prod_{i=1}^r \sigma_i(\alpha) \right)^q$

In particolare se L/K non separabile $\Rightarrow \text{Tr}_{L/K}(\alpha) \equiv 0$

Dim: - L/K non sep $\Rightarrow \text{char } K = p$ e $q = p^e \rightarrow \text{Tr}_{L/K} = p^e \sum \sigma_i(\alpha) \equiv 0 \pmod{p}$

- $\alpha \in K$ allora $\sigma_i(\alpha) = \alpha \forall i = 1, \dots, r$ e $\begin{matrix} \text{Tr}_{L/K}(\alpha) = q \cdot r \cdot \alpha \checkmark \\ N_{L/K}(\alpha) = \alpha^{q \cdot r} \checkmark \end{matrix}$

- Altrimenti:

• $L = K(\alpha) \Rightarrow \begin{matrix} \text{Tr}_{L/K}(\alpha) = -C_1 = q \sum \sigma_i(\alpha) \\ N_{L/K}(\alpha) = (-1)^n C_n = \left(\prod \sigma_i(\alpha) \right)^q \end{matrix}$

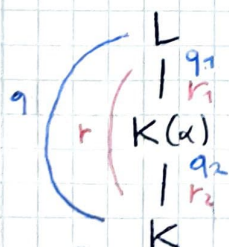
• $[L:K(\alpha)] = s = q_1 \cdot r_1, [K(\alpha):K] = q_2 \cdot r_2$ e $q = q_1 q_2, r = r_1 r_2$

Allora:

$$\begin{aligned} \text{Tr}_{L/K}(\alpha) &= q_1 \cdot r_1 \cdot q_2 \left(\sum_{i=1}^{r_2} \tau_i(\alpha) \right) \text{ dove } \tau_i: K(\alpha) \rightarrow \bar{K} \\ &= q \left(\sum_{i=1}^r \sigma_i(\alpha) \right) \end{aligned}$$

ma τ_i si estende a L in r_2 modi

$$N_{L/K}(\alpha) = \left(\left(\prod_{i=1}^{r_2} \tau_i(\alpha) \right)^{q_1} \right)^{q_2 \cdot r_2} = \left(\prod \sigma_i(\alpha) \right)^q$$



$\Rightarrow$ [Cor] L/K normale: $\text{Tr}_{L/K}(\alpha) = \text{Tr}_{L/K}(\sigma(\alpha))$

$$N_{L/K}(\alpha) = N_{L/K}(\sigma(\alpha))$$

$$\forall \sigma \in \text{Aut}(L)$$

Cor: $K \subseteq L \subseteq M$ bene $\Rightarrow \text{Tr}_{M/K} = \text{Tr}_{L/K} \circ \text{Tr}_{M/L}$
 $N_{M/K} = N_{L/K} \circ N_{M/L}$

Dim: $\begin{matrix} M \\ \text{m} \mid \{T_i\} \\ L \\ \text{n} \mid \{\bar{\gamma}_j\} \\ K \end{matrix} \quad \begin{array}{l} \forall j \text{ sia } \bar{\gamma}_j \text{ estensione di } \gamma_j \text{ a } M \\ \Rightarrow \text{Hom}(M, K) = \bigcup_j \bar{\gamma}_j \text{Hom}_L(M, L) \\ \text{Allora } q = [M:K]_i = [M:L]_i [L:K]_i = q_1 \cdot q_2 \end{array}$

Troviamo: $\text{Tr}_{M/K}(\alpha) = q \sum_i \sigma_i(\alpha) = q \sum_i \sum_j \bar{\gamma}_j \circ T_i(\alpha) =$
 $= q_1 \sum_j q_2 \bar{\gamma}_j \left(\sum_i T_i(\alpha) \right) = \text{Tr}_{L/K}(\text{Tr}_{M/L}(\alpha))$

Cor2: L/K finita allora:

- 1) L/K separabile $\Leftrightarrow \text{Tr}_{L/K} : L \rightarrow K$ e non banale (quindi surz)
- 2) L/K separabile $\Rightarrow \text{Tr} : L \times L \rightarrow K$ bilineare, simmetrica e non degenera
 $(x, y) \quad \text{Tr}_{L/K}(xy)$
 e induce un isomorfismo $\varphi : L \xrightarrow{x} \hat{L} = \text{Hom}(L, K)$
 $\text{Tr}(x \cdot)$

Dim: $1/K$ già visto
 $\Rightarrow L/K$ separabile con $[L:K] = r \rightarrow \sigma_1, \dots, \sigma_r$ immersioni, allora
 $\text{Tr}_{L/K} = \sigma_1 + \dots + \sigma_r$ dove $\sigma_i : L^* \rightarrow K^*$ sono caratteri distinti
 $\rightarrow$ [Artin] σ_i lin indep e Tr NON BANALE.

2) Sia $\varphi : \ker \varphi = \{x \in L : \text{Tr}(xL) = 0\} = \{0\}$. Infatti
 $x \neq 0 : xL = L \rightarrow \text{Tr}(xL) = \text{Tr}(L) \neq 0$ per (*)

$\rightarrow \varphi$ mappa lineare invertibile fra sp. vett. finiti con lo stesso dim $\rightarrow$ ISO

Quindi $\hat{L} \stackrel{(*)}{=} \{\text{Tr}_{L/K}(x \cdot) \mid x \in L\}$

Cor: L/K separabile finita con $\{x_1, \dots, x_n\}$ K -base di L

$\Rightarrow \exists! \{y_1, \dots, y_n\}$ base di L/K t.c. $\text{Tr}_{L/K}(x_i y_j) = \delta_{ij}$
 (base duale)

Dim: $\{x_1, \dots, x_n\}$ base di $L/K \rightarrow \{\hat{y}_1, \dots, \hat{y}_n\}$ base duale di $\{x_i\}$
 t.c. $\hat{y}_j(x_i) = \delta_{ij}$

Ma (*) $\exists y_i$ t.c. $\hat{y}_i = \text{Tr}(y_i \cdot) \rightarrow$ TROVO $y_1, \dots, y_n$ che rispettano

Inoltre y_i lin. indipendenti (perché $\{\varphi(y_i)\}$ lin indep)

* TEOREMA 90 DI HILBERT

04/30

Teo: L/k ciclica finita, $G = \text{Gal}(L/k) = \langle \sigma \rangle$ e sia $\alpha \in L$

1) $N_{L/k}(\alpha) = 1 \Leftrightarrow \exists \beta \in L$ t.c. $\alpha = \beta / \sigma(\beta)$

2) $\text{Tr}_{L/k}(\alpha) = 0 \Leftrightarrow \exists \beta \in L$ t.c. $\alpha = \beta - \sigma(\beta)$

Dim: 1) $(\Leftarrow)$ Supponiamo $N_{L/k}(\beta) = N_{L/k}(\sigma(\beta)) \rightarrow N_{L/k}(\alpha) = 1$

$(\Rightarrow)$ $\alpha \in L$ t.c. $N_{L/k}(\alpha) = 1 = \alpha \cdot \sigma(\alpha) \cdots \sigma^{n-1}(\alpha)$ ($[L:k] = n$)

Consideriamo $\chi = 1 + \alpha\sigma + \alpha\sigma(\alpha)\sigma^2 + \cdots + \alpha\sigma^2(\alpha) \cdots \sigma^{n-2}(\alpha)\sigma^{n-1}$
e non banale per il Teo d'indip dei caratteri ($\sigma^i: L^* \rightarrow L^*$)

$\Rightarrow \exists \gamma \in L^*$ tale che $\beta = \chi(\gamma) \neq 0$

Voglio dimostrare che $\alpha\sigma(\beta) = \beta$, allora:

$\sigma(\beta) = \sigma(\chi(\gamma)) = \sigma(\gamma) + \sigma(\alpha)\sigma^2(\gamma) + \cdots + \sigma(\alpha)\sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha) \sigma^n(\gamma)$
 $\boxed{\sigma^n(\gamma)} = \gamma$

$\alpha\sigma(\beta) = \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha)\gamma$
 $= N_{L/k}(\alpha) = 1$
 $= \chi(\gamma) = \beta$

2) $(\Leftarrow)$ $\text{Tr}(\beta - \sigma(\beta)) = \text{Tr}(\beta) - \text{Tr}(\sigma(\beta)) = 0 \checkmark$

$(\Rightarrow)$ $\alpha \in L$ e $0 = \text{Tr}_{L/k}(\alpha)$ dove $\text{Tr} = \sum_{i=0}^{n-1} \sigma^i$ non banale (Artin)
e quindi $\exists \gamma \in L: \text{Tr}_{L/k}(\gamma) \neq 0$

Sia $\beta = \frac{1}{\text{Tr}_{L/k}(\gamma)} ((\alpha\sigma(\gamma)) + (\alpha\sigma(\alpha))\sigma^2(\gamma) + \cdots + (\alpha\sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\gamma))$

Allora: $\sigma(\beta) = \frac{1}{\text{Tr}_{L/k}(\gamma)} (\sigma(\alpha)\sigma^2(\gamma) + (\sigma(\alpha) + \sigma^2(\alpha))\sigma^3(\gamma) + \cdots + (\sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha))\gamma)$
 $= -\alpha$

e $\beta - \sigma(\beta) = \frac{1}{\text{Tr}_{L/k}(\gamma)} (\alpha(\sigma(\gamma) + \sigma^2(\gamma) + \cdots + \sigma^{n-1}(\gamma)) - (-\alpha)\gamma) = \alpha$

* Hilbert 90 COOMOLOGICO

Sia $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ (1) esatta con A, B, C gruppi abeliani
t.c. G agisce su em via molt a sx

$\mathbb{Z}[G]$ -moduli: $\{ \sum_{\sigma \in G} a_\sigma \cdot \sigma \mid a_\sigma \in \mathbb{Z} \}$

Detto $A^G = \{ a \mid a^\sigma = a \ \forall \sigma \in G \}$ allora (1) induce

$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$ esatto a sx (*)

ex [in generale l'esattezza a dx non si conserva]

$1 \rightarrow \langle \zeta_n \rangle \hookrightarrow \mathbb{Q}^* \xrightarrow{\nu} \mathbb{Q}^*_{\zeta_n} \rightarrow 1$ (1*)
 ζ_n ζ_n

e sia $G = \text{Gal}(\mathbb{Q}/k)$ dove $k = \mathbb{Q}(\zeta_n)$

Allora: $\langle \zeta_n \rangle^G = \langle \zeta_n \rangle$ perché G è $\langle \zeta_n \rangle$ in modo banale

$$\overline{\mathbb{Q}}^{\times G} = K^{\times} \text{ per definizione di } G$$

allora:

$$(1^*) \text{ induce } 1 \rightarrow \langle \zeta_n \rangle \rightarrow K^{\times} \xrightarrow{U^G} K^{\times} \text{ dove}$$

$U^G = U|_{K^{\times}}$ non è surgettiva (in $K^{\times}$ non ho tutte le radici n -esime!)

Vogliamo completare $(*)$ in modo che rimanga esatta
Definiamo:

$$Z^1(G, A) = \{ f: G \rightarrow A \mid f(\sigma \circ \tau) = f(\sigma) \circ f(\tau) \quad \forall \sigma, \tau \} \text{ gruppo degli 1-cocchi}$$

omomorfismi cocicli

$$\bullet Z^1(G, A) = \text{Hom}(G, A) \Leftrightarrow G \text{ agisce su } A \text{ banalmente}$$

$$B^1(G, A) = \{ f: G \rightarrow A \mid \exists a \in A \text{ t.c. } f(\sigma) = \sigma^{-1}(a) \cdot a \quad \forall \sigma \} \text{ 1-cobordi}$$

$(\hookrightarrow Z^1(G, A))$

$$\text{ed infine } H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}$$

Teo [Hilbert 90 coomologico]

$$L/K \text{ di Galois finite, } G = \text{Gal}(L/K) \text{ allora: } H^1(G, L^{\times}) = \{1\}$$

$$H^1(G, L) = \{0\}$$

Dim: $\bullet f: G \rightarrow L^{\times}$ 1-cociclo $\Rightarrow f(\sigma \circ \tau) = f(\sigma) \circ f(\tau)$
e $\sum_{\sigma} f(\sigma) \sigma$ non banale per indep. caratteri

Quindi $\exists \gamma \in L^{\times} : \beta = \sum_{\sigma} f(\sigma) \sigma(\gamma) \neq 0$

Ten: $f(\sigma) = \sigma^{-1}(\beta) \beta$

$$\begin{aligned} \sigma(\beta) &= \sum_{\tau} \sigma f(\tau) \sigma \circ \tau(\gamma) = \sum_{\tau} f(\sigma)^{-1} f(\sigma \circ \tau) (\sigma \circ \tau)(\gamma) \\ &= f(\sigma)^{-1} \sum_{\tau} f(\tau) \tau(\gamma) = f(\sigma)^{-1} \beta \Rightarrow \text{ten} \end{aligned}$$

Ovvero, ogni 1-cociclo è un 1-cobordo

$\bullet f: G \rightarrow L$ 1-cociclo $\Rightarrow f(\sigma \circ \tau) = f(\sigma) + \sigma f(\tau)$

Esiste c t.c. $\text{Tr}_{L/K}(c) \neq 0 \Rightarrow a = \frac{1}{\text{Tr}_{L/K}(c)} \sum_{\tau} f(\tau) \tau(c)$

$$\begin{aligned} \text{Ma allora } \sigma(a) &= \frac{1}{\text{Tr}_{L/K}(c)} \sum_{\tau} \sigma f(\tau) \sigma \circ \tau(c) = \frac{1}{\text{Tr}_{L/K}(c)} \sum (f(\sigma \circ \tau) - f(\sigma)) \sigma \circ \tau(c) \\ &= a - f(\sigma) \Rightarrow f(\sigma) = a - \sigma(a) \end{aligned}$$

Cor: Hilbert 90 classica

Dim: $f: G \rightarrow L^{\times}$ t.c. $f(\text{id}) = 1, f(\sigma) = \alpha$ e $f(\sigma^i) = \alpha \sigma(\alpha) \dots \sigma^{i-1}(\alpha)$
è un 1-cociclo infatti se $N_{L/K}(\alpha) = 1$:

$$\begin{aligned} f(\sigma^i \circ \sigma^j) &= \alpha \sigma(\alpha) \dots \sigma^{i+j-1}(\alpha) = \alpha \sigma(\alpha) \dots \sigma^{i-1}(\alpha) \sigma^i(\alpha \sigma(\alpha) \dots \sigma^{j-1}(\alpha)) \\ &= \alpha \sigma(\alpha) \dots \sigma^{i+j-1}(\alpha) [N_{L/K}(\alpha)] \alpha \end{aligned}$$

$\Rightarrow \exists \beta: \alpha \cdot f(\sigma) = \sigma^{-1}(\beta) \beta$

* ESTENSIONI CICLICHE

Teo [KUMMER - estensioni cicliche] K campo char $\neq n$ e $\zeta_n \in K$

1) L/K ciclica di grado $n \Rightarrow \exists \alpha \in L$ t.c. $L = K(\alpha)$ ed inoltre
 $N_{L/K}(\alpha) = \alpha^n - c \in K[x]$

2) $L = K(\alpha)$, α radice n -esima di $c \in K$ allora
 L/K ciclica di grado $d|n$ con $d = \min \{k \mid \alpha^k \in K\}$

Dim (1): L/K ciclica, $G = \langle \sigma \rangle = \text{Gal}(L/K)$ e applico H90

$$\zeta = \zeta_n \in K \rightarrow N_{L/K}(\zeta_n^{-1}) = \zeta_n^{-n} = 1 \xrightarrow{\text{H90}} \zeta_n^{-1} = \frac{\alpha}{\sigma(\alpha)} \quad \alpha \in L$$

Ovvero $\sigma(\alpha) = \zeta \alpha$

da cui $G\alpha = \{ \sigma^i(\alpha) \} = \{ \alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha \}$
 e poiché char $\neq n \rightarrow x^n - 1$ separabile $\Rightarrow |G\alpha| = n$

$$\Rightarrow L = K(\alpha) \quad ([K(\alpha):K] = n)$$

Inoltre $N_{L/K}(\alpha) = \prod (x - \zeta^i \alpha) = x^n - \alpha^n \in K[x] \rightarrow \alpha^n \in K$
 Oppure $\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta\alpha)^n = \alpha^n \rightarrow \mu_{\alpha} | x^n - \alpha^n = (x - \alpha)^n$

(2): Sia $\alpha \neq 0, \alpha \in \overline{K}$ t.c. $f(x) = x^n - c$ e $f(\alpha) = 0$

$\Rightarrow$ le radici di f in $K = \{ \alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha \}$: quindi

$L = K(\alpha)/K$ è - normale (Cds di $x^n - c$)
 - separabile (char $\neq n \rightarrow f$ separabile e $\mu_{\alpha} | f$)
 quindi è di Galois

$$\Rightarrow \mu_{\alpha}(x) \mid \prod (x - \zeta^i \alpha) \Rightarrow \sigma(\alpha) = \zeta^{i_{\sigma}} \alpha \quad \forall \sigma \in \text{Gal}(L/K)$$

$$\Rightarrow \text{Gal}(L/K) \xrightarrow{\sigma} \langle \zeta^{i_{\sigma}} \rangle \text{ omom. iniettivo} \rightarrow L = K(\alpha) : \sigma(\alpha) = \zeta^{i_{\sigma}} \alpha \Rightarrow \sigma \equiv \tau$$

$$\Rightarrow G = \text{Gal}(L/K) \xrightarrow{\sigma} \langle \zeta \rangle \cong \mathbb{Z}/n\mathbb{Z} \Rightarrow G \cong \mathbb{Z}/d\mathbb{Z} \quad d|n$$

Ma allora: $G = \langle \sigma \rangle$ dove $d = \text{ord}(\sigma) \equiv \text{ord}(\zeta^{i_{\sigma}})$

$$\Rightarrow \sigma(\alpha^d) = (\sigma(\alpha))^d = (\zeta^{i_{\sigma}} \alpha)^d = (\zeta^{i_{\sigma}})^d \alpha^d = \alpha^d \in K$$

⚠ Si poteva evitare l'uso di H90 e dimostrare il teorema via algebre lineari

$\sigma: L \rightarrow L$ lineare e $p_{\sigma}(x) = x^n - 1$ pol. caratteristico di σ di ordine n

$$\Rightarrow p_{\sigma}(x) = \prod (x - \zeta^i) \text{ e } \zeta^i \text{ tutti distinti se char } K \neq n$$

Ma allora $p_{\sigma}(x) = p_{\sigma}(x)$.

Inoltre ζ autovettore di $\sigma \Rightarrow \exists \alpha$ t.c. $\sigma(\alpha) = \zeta \alpha$

Teo [Artin-Schreier] K campo, $\text{char } K = p$ (quindi $1 = \sum_{i=0}^{p-1} 1 \in K$)

1) L/K ciclica di grado $p \Rightarrow L = K(\alpha)$ con $N_\alpha(x) = x^p - x - c$

2) $L = K(\alpha)$ con α radice di $x^p - x - c \Rightarrow K(\alpha)$ ciclica di $\text{deg } 1, p$

(ovvero $x^p - x - c$ è irriducibile o completamente fattorizzabile)

Dim: 1) L/K ciclica di grado p e $\text{Tr}(-1) = -(1+1+\dots+1) = -p = 0$

$\Rightarrow$ esiste $\alpha \in L$: $\sigma(\alpha) - \alpha = 1$ ovvero $\sigma^p(\alpha) = \alpha + 1$

Sia $G = \langle \sigma \rangle = \text{Gal}(L/K)$: $G\alpha = \{\sigma^i(\alpha)\} = \{\alpha, \alpha+1, \dots, \alpha+p-1\}$
e $|G\alpha| = p \Rightarrow L = K(\alpha)$

Dimostriamo che $N_\alpha(x) = x^p - x - c \Rightarrow c = \alpha^p - \alpha \in K$

Ora:

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha^p) - \sigma(\alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha \in K$$

quindi vale lo tesi

2) $L = K(\alpha)$ con $\alpha^p - \alpha - c = 0$, $c \in K$. Allora $f = x^p - x - c$

$\alpha+1$ radice di f ($(\alpha+1)^p - (\alpha+1) - c = \alpha^p - \alpha - c = 0$)

$\Rightarrow$ i radici di f $= \{\alpha, \alpha+1, \dots, \alpha+p-1\}$, quindi

- f separabile (p radici distinte)
- $L = K(\alpha)$ e $\{\alpha+i\}$ e-cts di $f \rightarrow$ normale $\} L/K$ di Galois

So che $N_\alpha(x) = \prod_{i \in I} (x - (\alpha+i)) \in K[x]$

$\Rightarrow \text{Tr}_{L/K}(\alpha) = \sum_{i \in I} \alpha+i = |I|\alpha + j = (\deg N_\alpha)\alpha + j \in K$
da cui necessariamente $(\deg N_\alpha)\alpha \in K \rightarrow \begin{cases} d=0 \\ \alpha \in K \end{cases} (d=p)$

Cioè: $-\alpha \in K \Rightarrow L = K$ ciclica di $\text{deg} = 1$; oppure
 $-d=p \Rightarrow N_\alpha = f$ e $[L:K] = p \rightarrow$ ciclica

$\triangle$ Anche qui potremmo usare H90

$\sigma: L \rightarrow L$ di ordine p e $P_\sigma(x) = x^p - 1 = (x-1)^p$
 $N_\sigma(x) = (x-1)^d$ con $d \leq p$ $d > 1$

$\Rightarrow \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ blocco di Jordan di dimensione d e $\{v_1, \dots, v_d\}$ base

$\Rightarrow \sigma(v_1) = v_1$, $\sigma(v_i) = v_i + v_{i-1}$ ma allora:

$$\sigma\left(\frac{v_2}{v_1}\right) = 1 + \frac{v_2}{v_1} \text{ e pongo } \frac{v_2}{v_1} = \alpha \rightarrow \sigma(\alpha) = 1 + \alpha$$

TEO [Artin] K campo, $i \in \bar{K}$ ($i^2 = -1$) $[\bar{K} : K] < +\infty \Rightarrow \bar{K} = K(i)$
 Inoltre se $\bar{K}/K$ è non banale $\Rightarrow \text{char } K = 0$

05/02

Dim: $\bar{K}/K$ normale (Cds di $\exists f \in K[x] \text{ p.p.}$)
 separabile: $\text{char } K = 0 \rightarrow$ ovvio
 $\text{char } K = p: K^{p^{-\infty}} \subset \bar{K} \text{ e } [K^{p^{-\infty}} : K] = \begin{cases} 1 \\ +\infty \end{cases}$
 $\rightarrow K = K^{p^{-\infty}}$ pu fatto ✓

$\Rightarrow \bar{K}/K$ di Galois e $K \subseteq K(i) \subseteq \bar{K} \rightarrow K(i)/K$ di Galois

Suo alone $G = \text{Gal}(\bar{K}/K(i))$ voglio dimostrare che è banale

G non banale $\Rightarrow \exists$ primo t.c. $e \mid |G|$ e ha $H < G$
 $|H| = e$
 $\Rightarrow L = \bar{K}^H$ con $\bar{K}/L$ di Galois ciclica

[Se $\text{char } K = e$] per Artin-Schreier $\exists a \in L: \bar{K} = L(a)$
 ed inoltre α rad di $x^p - x - c$

Facciamo vedere che $x^p - x - c$ rad in $L[x] \forall c$
 Sia $T: \bar{K} \rightarrow \bar{K}$ $\alpha \mapsto \alpha^p - \alpha$ è surgettiva
 $[L(a):L] = 1$
 se $\alpha^p - \alpha - c = 0$ e mostriamo che $\text{Tr}_{\bar{K}/L} \circ T = T|_L \circ \text{Tr}_{\bar{K}/L}$
 $\text{Tr}_{\bar{K}/L}(T(\alpha)) = \text{Tr}_{\bar{K}/L}(\alpha^p - \alpha) = (\text{Tr}_{\bar{K}/L}(\alpha))^p - \text{Tr}_{\bar{K}/L}(\alpha) \checkmark$
 $\rightarrow T|_L$ è surgettiva $\rightarrow x^p - x - c$ riducibile in L

[Se $\text{char } K \neq e$] $\exists c \in L \leftarrow ([L(\zeta_e):L] \mid e \mid [L(\zeta_e):L] \leq e-1)$

$\Rightarrow \exists a \in \bar{K}$ t.c. $L(a) = \bar{K}$, $N_a(x) = x^e - c$
 Kummer

Come sopra: $\alpha^e = a: N_{\bar{K}/L}(\alpha)^e = N_{\bar{K}/L}(\alpha^e) = N_{\bar{K}/L}(a) = (-1)^e(-c) = (-1)^{e+1}c$
 $2 \nmid e \Rightarrow N_{\bar{K}/L}(\alpha) \in L$ radice di $x^e - c$
 (con perché lo supponiamo irr.)
 $e = 2 \Rightarrow N_{\bar{K}/L}(\alpha)^2 = -c \in L^{\wedge 2}$ e $i \in L \rightarrow c \in L^{\wedge 2}$ (am)

$\rightarrow |G| = 1 \rightarrow \bar{K}/K(i)$ banale $\Rightarrow \bar{K} = K(i)$

• $\bar{K} \neq K$ mostriamo $\text{char } K = 0: K \subsetneq K(i) = \bar{K}$,
 quindi $i \notin K$, ovvero -1 non è un quadrato in K

Ora oremo che $N_{\bar{K}/K}(a+ib) = a^2+b^2$ e inoltre $\exists x+iy: (x+iy)^2 = a+ib$

$\rightarrow a^2+b^2 = N_{\bar{K}/K}(a+ib) = (N_{\bar{K}/K}(x+iy))^2 = (x^2+y^2)^2$ la somma di $\square$ è un $\square$

Se $\text{char } K = p \Rightarrow -1 \equiv p-1 \equiv \sum_{i=1}^{p-1} 1$ è un quadrato, ovv.

Qss: $c \in \bar{K}$ e $\alpha \in \bar{K}$, $N\alpha = \alpha^e - c$ con $c = L^{\wedge 2}$
 con $\exists \alpha \in K$ è irriducibile

$L(\sqrt[e]{c})$

$\Leftrightarrow [K(a):K] = e \Leftrightarrow \alpha^d \notin K \forall d \mid e \Leftrightarrow c \notin K^{\wedge p}$

L

$\exists \exists \nexists K \leftarrow$ falso: $x^4 + 4 \in \mathbb{R}[x]$

TEO [Fondamentale dell'algebra - Artin] $\mathbb{C}$ è algebricamente chiuso

Dim: 1. $z \in \mathbb{C} \Rightarrow \exists w \in \mathbb{C} : w^2 = z$. Sia $z = x+iy$ e $w = a+ib$
Allora $x+iy = z = w^2 = (a+ib)^2 = a^2 - b^2 + i(2ab)$ e

$$x^2 + y^2 = N(w^2) = (a^2 + b^2)^2 \in \mathbb{R}^+$$

$$\Rightarrow \begin{cases} a^2 + b^2 = \pm \sqrt{x^2 + y^2} \\ a^2 - b^2 = x \end{cases} \rightarrow \begin{cases} a^2 = \frac{1}{2} (x + \sqrt{x^2 + y^2}) \geq 0 \\ b^2 = \frac{1}{2} (-x + \sqrt{x^2 + y^2}) \geq 0 \end{cases} \quad a, b \in \mathbb{R}$$

2. $\mathbb{C}$ alg chiuso $\Leftrightarrow \mathbb{C}$ alg su $\mathbb{C} \rightarrow \mathbb{C} \in \mathbb{C} \Leftrightarrow \forall \mathbb{C} \subset L$ finita $\Rightarrow L = \mathbb{C}$

Baske (6) per $\mathbb{C} \subset L$ di Galois (su $\mathbb{R}$), finite. $[L:\mathbb{R}] = 2^k m, (m, 2) = 1$
 $\mathbb{C} \subset L \rightarrow k \geq 1$

H 2-Sylow di $G = \text{Gal}(L/\mathbb{R})$

$\Rightarrow L^H/\mathbb{R}$ estensione di grado dispari finita e sep

$\rightarrow L^H = \mathbb{R}(\alpha)$ con p_α irreducibile su $\mathbb{R}$ e grado dispari
ASS: $\exists$ polinomi di deg dispari hanno almeno 1 radice su $\mathbb{R}$
(continuità + $\lim_{x \rightarrow \pm \infty} f(x) = \pm \infty$)

$\Rightarrow L^H = \mathbb{R}$ cioè $m = 1 \rightarrow [L:\mathbb{R}] = 2^k$

Allora $L/\mathbb{C}$ di Galois e $\text{Gal}(L/\mathbb{C})$ è un 2-gruppo e $k > 1$

$\Rightarrow \exists N \triangleleft \text{Gal}(L/\mathbb{C})$ dove $|N| = 2^{k-2}$ (indice 2)

Allora $[L^N:\mathbb{C}] = 2$ e $L^N = \mathbb{C}(\alpha)$ con p_α di deg 2
irreducibile
 $\rightarrow$ an per 1.

Es: $\overline{\mathbb{Q}}, \alpha \in \overline{\mathbb{Q}}/\mathbb{Q}$ Allora: $\bullet \exists E$ sotto campo max di $\overline{\mathbb{Q}}$ t.c. $\alpha \notin E$
 $\bullet \forall E \subseteq K$ finito $\Rightarrow K/E$ ciclica di grado p^n
dove $p = [\mathbb{Q}(\alpha):\mathbb{Q}]$
 $\bullet \text{Gal}(\overline{\mathbb{Q}}/E) \cong \mathbb{Z}_p \vee \mathbb{Z}_{p^2}$

Sol: $\bullet \mathcal{F} = \{K \subset \overline{\mathbb{Q}} : \alpha \notin K\} \ni \mathbb{Q}$, induttivo $\rightarrow \exists E$ max in $\mathcal{F}$
 $\bullet E(\alpha)/E$ è normale: se $p_\alpha(x) = \prod (x - \alpha_i)$ e $\phi_i: E(\alpha) \rightarrow \overline{\mathbb{Q}}$, $\phi_i|_E = \text{id}$

Ma allora $\phi_i(E(\alpha)) = E(\alpha_i)$ e $[E(\alpha_i):E] = n$ se $\alpha_i \notin E$
 $\rightarrow \alpha \notin E(\alpha_i) \rightarrow$ an pm max di E in $\mathcal{F} \rightarrow E(\alpha_i) = E \checkmark$

Inoltre $E \subset F \subset E(\alpha): F = E, F = E(\alpha)$ pm max di E in $\mathcal{F}$
 $\text{Gal}(E(\alpha)/E)$ non ha sgr propri $\rightarrow$ ciclico di ordine p

Sia $K: E$ finita: a meno di $\tilde{K} = U \circ K$ supposto K di Galois
 $\Rightarrow E \subset E(\alpha) \subset K$ poiché $E(\alpha) \subset L \forall E \subset L \subset K \rightarrow \exists H < G$ t.c.
H contiene tutti i sgr propri di G

$\rightarrow x \in G \setminus H \Rightarrow G = \langle x \rangle$: ciclico finito
e poiché ho un unico sgr max vale $|G| = p^n$

K non normale $\rightarrow \tilde{K}/E$ ciclico $\Rightarrow K/E$ normale

$\bullet \text{Gal}(\overline{\mathbb{Q}}/E) = \bigcup_{\text{Artin}} \mathbb{Z}_{p^n}$

$[\overline{\mathbb{Q}}:E] = +\infty \Rightarrow \text{Gal}(\overline{\mathbb{Q}}/E) = \varprojlim \text{Gal}(F/E) = \varprojlim \mathbb{Z}_{p^n} \cong \mathbb{Z}_p$

Def: un gruppo G si dice risolubile se ammette una catena di sottogruppi

05/07

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \dots \triangleleft G_2 \triangleleft G_1 = G \quad \text{t.c. } G_i/G_{i+1} \text{ è abeliano}$$

[ammette una serie (sub)normale a quozienti abeliani]

- ex:
- G abeliano $\Rightarrow G$ risolubile
 - G p-gruppo finito $\Rightarrow G$ risolubile

Oss: G risolubile $\Rightarrow$ ogni serie subnormale a quozienti abeliani può essere raffinata ad una serie subnormale a quozienti ciclici

[segue dal teo di struttura dei gruppi abeliani finiti]

Def: G gruppo: $DG = [G, G] = \langle [g, h] = ghg^{-1}h^{-1} \mid g, h \in G \rangle$
gruppo dei commutatori / gruppo derivato

- Prop:
- G abeliano $\Leftrightarrow DG$ è banale
 - $DG \triangleleft G$ ed è il più piccolo sottogruppo normale di G con G/DG abeliano

$\rightarrow$ definiamo induttivamente: $D^n G = D(D^{n-1} G) = [D^{n-1} G, D^{n-1} G]$
 $D^0 G := G$

Ma quindi, per la PROP:

$$G = D^0 G \triangleright DG \triangleright D^2 G \triangleright \dots \triangleright D^n G \triangleright \dots$$

$\xrightarrow{\text{termina?}}$

Prop: G risolubile $\Leftrightarrow \exists n: D^n G = \{e\}$

Dim: ($\Leftarrow$) ovvio per la PROP

($\Rightarrow$) Supponiamo G sia risolubile con serie $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$

Allora: G/G_1 abeliano $\xrightarrow{\text{PROP}} DG \subset G_1$

G_i/G_{i+1} abeliano $\xrightarrow{\text{PROP}} DG_i \subset G_{i+1}$

Per induzione dimostriamo che $D^i G \subset G_i$ (P.I. $G_{i+1} \triangleright DG_i \triangleright D(D^i G)$)

Quindi $D^n G \subset G_n = \{e\} \rightarrow D^n G = \{e\}$

Prop: G gruppo, $H \triangleleft G$:

- G risolubile $\Rightarrow H$ risolubile (1)
- $[G \text{ risolubile} \Leftrightarrow H, G/H \text{ risolubile}]$ (2)

Dim: (1) $\exists n$ t.c. $D^n G = \{e\} \rightarrow D^n H \subset D^n G = \{e\} \rightarrow D^n H = \{e\}$

(2) Supponiamo G risolubile: dico per ipotesi G/H risolubile
Sia n : $D^n G = \{e\}$, voglio dire $D^n(G/H) = \{e\}$

{Guardo $\pi: G \rightarrow G/H$ omomorfismo: $\pi(D^i G) = D^i \pi(G)$ }
(per induzione)

Supponiamo $H, G/H$ risolubili:

$\exists h, m: D^h H = D^m(G/H) = \{e\}$, ma allora

$\pi(D^m G) = D^m(G/H) = \{e\} \rightarrow D^m G \subset H$
e applicando D^h trovo $D^{m+h} G \subset D^h H = \{e\}$

(Si vede anche con la serie di H e il sollevamento della serie di G/H).

Es: S_n è risolubile $\Leftrightarrow n < 5$

- $DS_n = A_n$ se $n \geq 3$
 $D^2 S_n = D A_n = A_n$ se $n \geq 5$ ($(abc) = [(abc), (ade)]$)

$\rightarrow n \geq 5 \rightarrow S_n$ NON è risolubile e ho:

- $S_2 = \mathbb{Z}/2\mathbb{Z}$
- $\{e\} \triangleleft A_3 \triangleleft A_3 \rtimes \mathbb{Z}/2\mathbb{Z} = S_3$
- $\{e\} \triangleleft K \triangleleft A_4 \triangleleft S_4$
4 3 2

• ESTENSIONI RISOLUBILI

Def: L/K si dice risolubile se $\exists E \supset L$ t.c. E/K di Galois e $\text{Gal}(E/K)$ risolubile
finita

Prop: 1) L/K risolubile $\Rightarrow L/K$ separabile

$$K \subset L \subset E$$

2) Se L/K è risolubile e $F \in L \Rightarrow F/K$ risolubile (avv)

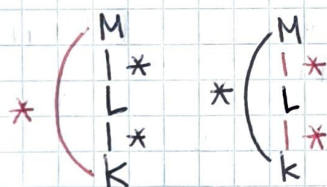
3) Se L/K è risolubile $\Leftrightarrow \tilde{L} =$ chiusura normale di L/K
 $\text{Gal}(\tilde{L}/K)$ è risolubile

Dim: 1) L/K risolubile $\Rightarrow \exists E$ t.c. $L \subset E$ e E/K di Galois
 quindi E/K separabile $\xrightarrow{\text{Torri}} L/K$ separabile

3) $(\Leftarrow)$ avv
 $(\Rightarrow) E/K$ di Galois $\Rightarrow \tilde{L} \subset E$ quindi $\text{Gal}(\tilde{L}/K) \cong \frac{\text{Gal}(E/K)}{\text{Gal}(E/\tilde{L})}$
 ovvero risolubile in quanto
 quoziente di un gruppo risolubile

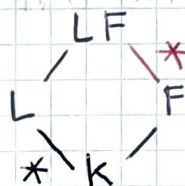
* PROPRIETÀ DELLE ESTENSIONI RISOLUBILI

① TORRI



M/K ris $\Leftrightarrow M/L, L/K$ risolubili

② SHIFT



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

③ COMPOSTO (T+S)

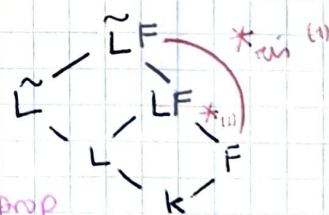
$L/K, F/K$ ris

$\Downarrow$
 LF/K risolubile



Dim: (2) Per la prop, a meno di sostituire L con $\tilde{L}$,
 posso supporre L/K normale

$\rightarrow L/K$ ris di Galois $\Rightarrow LF/F$ è di Galois
SHIFT
 e $\text{Gal}(LF/F) < \text{Gal}(L/K)$ quindi risolubile
(1) $\Rightarrow$ (2) per la prop



(1) M/K risolubile $\Leftrightarrow \text{Gal}(\tilde{M}/K)$ risolubile $\Rightarrow \text{Gal}(\tilde{M}/L)$ risolubile

$M/L, L/K$ risolubili:

voglio M/K ris $\Leftrightarrow \tilde{M}$ ha $\text{Gal}(\tilde{M}/K)$ ris.

$\rightarrow M_L$ risolubile, L/K ris
(prop)

Oss: $\tilde{M} = \Pi_{\sigma} M$ $\sigma \in \text{Hom}_K(M, \bar{K})$



[Caso: $L/K, M/K$ normali] Th $\Rightarrow \text{Gal}(L/K)$

$\text{Gal}(\tilde{M}/L)$ risolubili (Gm $\cong H, G/H$ ris)

$\text{Gal}(L/K)$ risolubile per ipotesi. Dimostriamo l'altra.

$\forall \sigma \in \text{Hom}_K(M, \bar{K}) \rightarrow \sigma L = L$ poiché L/K normale

Allora $\sigma M / \sigma L = \sigma M / L$ $\text{Gal}(\sigma M / L) \cong \text{Gal}(M / L)$ risolubili

$\rightarrow \text{Gal}(\tilde{M}/L) \hookrightarrow \Pi_{\sigma} \text{Gal}(\sigma M / L)$ sgr di gruppo risolubile $\rightarrow$ risolubile

In generale



gen finito + induzione $[G_1 \times G_2 \text{ ris} \Rightarrow G_1, G_1 \times G_2 / G_1 \cong G_2 \text{ ris}]$

$L' =$ chiusura normale L/K
 $M' =$ chiusura normale M/L'

Per il caso $\uparrow$: M'/K risolubile e $M \subset M'$
 $\Rightarrow M/K$ risolubile

• ESTENSIONI RISOLUBILI PER RADICALI

Def: L/K finita si dice risolubile per radicali se esiste una estensione $E \supset L$ ed una catena di sottocampi

$K = E_0 \subset E_1 \subset \dots \subset E_n = E$ t.c. $E_{i+1} = E_i(\alpha)$ dove $\alpha \in$

α pure
enno ξ_m

1) radice di $x^n - a \in E_i$
con $\text{char } K \nmid n$

2) radice di $x^p - x - c \in E_i$
con $\text{char } K = p$

Oss: $-L/K$ risolubile per radicali
 $\Rightarrow L/K$ separabile

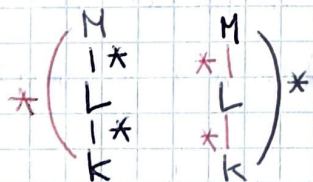
(ogni E_{i+1}/E_i separabile $\rightarrow E/K$ sep
e quindi L/K separabile)

$-L/K$ risolubile per radicali

$\Rightarrow \forall K \subset F \subset L, F/K$ risolubile per radicali

• PROPRIETA' DELLE ESTENSIONI RISOLUBILI PER RADICALI

① TORRI

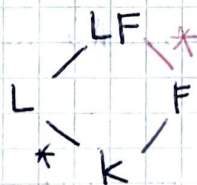


M/K ris per rad $\Rightarrow M/L, L/K$ ris per rad

$(\Rightarrow) L/K$ ovvio, $M/L = \frac{M}{L}$ per SHIFT (2)

$(\Leftarrow) E$ che trova da L/K : E/K ris per rad
e $M' = ME/E$ ris per rad (SHIFT) $\rightarrow M'/K \xrightarrow{\text{ris per rad}} M/K$

② SHIFT



③ COMPOSTO



Il traslato con F delle
catene di L/K e una
catena di LF/F

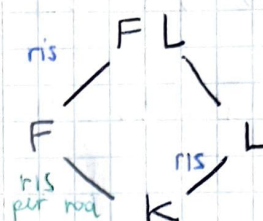
Teo: M/K finita e RISOLUBILE $\Leftrightarrow$ RISOLUBILE per RADICALI

05/03

Dim: $(\Rightarrow)$ L/K risolubile, posto rapporto di Galois, $\text{Gal}(L/K)$ risolubile

Sia $m = \prod_{\substack{p \mid [L:K] \\ p \neq \text{char } K}} p$ e $F = K(\zeta_m)$

Voglio dire FL/K ris per radicali
(tom): poiché $F = K(\zeta_m)$ basta FL/F ris per rad.



(sm:FT) FL/F risolubile + Galois. $G_0 = \text{Gal}(FL/F) \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$
serie subnormale e qm cicli di ordine primo

(Teo Galois) $F = F_0 \subset F_1 \subset \dots \subset F_n = LF$ dove $\text{Gal}(F_{i+1}/F_i) \cong G_i/G_{i+1}$
CICLICO DI ORDINE p
dove $p \mid [LF:F] \cdot [L:K]$

- $p = \text{char } K \xrightarrow{AS} F_{i+1} = F_i(\alpha)$ con $\alpha^p - \alpha - c = 0$
- $p \neq \text{char } K \rightarrow \exists p \in F + K : F_{i+1} = F_i(\alpha)$ con $\alpha^p - \alpha - c$

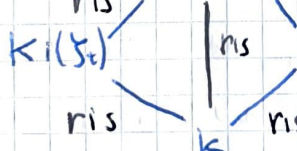
$\Rightarrow LF/F$ risolubile per radicali

$(\Leftarrow)$ L/K risolubile per radicali: $K = K_0 \subset K_1 \subset \dots \subset K_n = L$
dove $K_{i+1} = K_i(\alpha)$ e α radice di $x^n - a$ o $x^p - x - c$

Per dimostrare L/K risolubile $\rightarrow$ basta mostrare K_{i+1}/K_i risolubile

- K_{i+1}/K_i da AS $\Rightarrow \text{Gal}(K_{i+1}/K_i) \cong \mathbb{Z}/p\mathbb{Z}$ risolubile
- $K_{i+1} = K_i(\alpha)$ con $\alpha = \sqrt[p]{a}$ $a \in K_i$: se $\alpha = \zeta_m$ $\rightarrow K_{i+1}$ abeliana $\rightarrow$ ris.

Altrimenti: (*) $K_{i+1}(\zeta_p)$



(*) Kummer $\rightarrow \text{Gal}(K_{i+1}(\zeta_p)/K_i(\zeta_p)) \cong \mathbb{Z}/p\mathbb{Z}$
 $\Rightarrow K_{i+1}(\zeta_p)/K_i$ ris
 $\Rightarrow K_i(\alpha) = K_{i+1}/K_i$ ris

Cor: L'eq. generale di un polinomio di grado n e risolubile per radicali se e solo se $n \leq 4$

Dim: ris per radicali $\Leftrightarrow S_n$ risolubile $\Leftrightarrow n \leq 4$

Def: $\sigma \in S(\mathbb{F}_p)$ n' dice linear n esistono $a, b \in \mathbb{F}_p$ tali che

$$\sigma_{a,b}(x) = ax + b \quad \forall x \in \mathbb{F}_p, a \neq 0$$

$\mathbb{F}_p = \{ \sigma_{a,b} \mid \sigma_{a,b} \in S(\mathbb{F}_p) \}$ sottogruppo lineare con $|\mathbb{F}_p| = p(p-1)$

$G \leq S_p$ n' dice linear $\Leftrightarrow \exists \{1, \dots, p\} \rightarrow \mathbb{F}_p + c : G \hookrightarrow \mathbb{F}_p$

Prop: $\pi \in \text{Sp}$ p-ciclo: $N_{\text{Sp}}(\pi) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^* \cong F_p$

Dim: $|N_{\text{Sp}}(\pi)| = |Z_{\text{Sp}}(\pi)| \phi(p) = p(p-1)$, $\langle \pi \rangle \cap \text{Stab}_{N_{\text{Sp}}}(1) = \text{def} \langle \pi \rangle$

$\rightarrow N_{\text{Sp}}(\pi) \cong \langle \pi \rangle \rtimes \text{Stab}_{N_{\text{Sp}}}(1)$, wlog $\pi = (12 \dots p)$
 $\sigma \pi \sigma^{-1} = \pi^i$

Dato $\sigma \in \text{Stab}_{N_{\text{Sp}}}(1)$: $\sigma(1) = 1$
 $\sigma \pi \sigma^{-1}(1) = \sigma \pi(1) = \sigma(2) = \pi^i(1) = i+1$

$\rightarrow \text{Stab}_{N_{\text{Sp}}}(1) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}^*$
 $\sigma \mapsto \sigma(2)-1$

On $\pi = \sigma_{1,1}$ ($\pi(i) = i+1$): $\langle \pi \rangle = \{ \sigma_{1,b} \} \triangleleft F_p$

$\{1, \dots, p\} \xrightarrow{\sim} F_p$ allora $F_p \triangleleft N_{\text{Sp}}(\pi)$ e per ordine $F_p = N_{\text{Sp}}(\pi)$

Prop2: $\sigma \in F_p$ con almeno 2 punti fissi $\Rightarrow \sigma = \text{id}$

Dim: $\sigma = \sigma_{ab}(x) = ax+b = x$ con $a \neq 1 \rightarrow x = \frac{-b}{(a-1)}$

Se $a=1$: ha sol $\Leftrightarrow b=0$

Prop3: $G \triangleleft \text{Sp}$ che agisce transitivamente su $1, \dots, p$. Allora
 sono fatti equivalenti:

- G è lineare ($\Leftrightarrow G \triangleleft N_{\text{Sp}}(\pi)$ π p-ciclo)
- G è riducibile

Dim: (a) $\Rightarrow$ (b) G lineare $\Rightarrow G \triangleleft N_{\text{Sp}}(\pi)$ riducibile

(b) $\Rightarrow$ (a): basta far vedere che
 c'è un unico stir di ordine p in G (*)

$(G \triangleleft \text{Sp} \text{ trans} \rightarrow \pi \in G \xrightarrow{(*)} \pi \triangleleft G \rightarrow G \triangleleft N_{\text{Sp}}(\pi))$

Sia $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \text{def}$ a p-nucleo di ordine primo

1. $\forall i$ $G_i \triangleleft \text{Sp}$ transitivamente (induzione)

P.B: $i=0 \rightarrow \text{vero}$

P.I: G_{i-1} transitivo e concludo G_i hanno $B_1, \dots, B_t$ le orbite

$$\Rightarrow p = \sum_{j=1}^t |B_j| \quad \text{e} \quad |B_j| = \frac{|G_i|}{|\text{Stab}_{G_i}(x_j)|} \quad \text{se } B_j = \text{orb}(x_j)$$

Se che $\forall j, k \exists g \in G_{i-1} \text{ t.c. } g x_j = x_k$ allora:

$$\text{Stab}_{G_i}(x_j) \xleftrightarrow{1-1} \text{Stab}_{g G_{i-1} g^{-1}}(x_k) \quad G_i \triangleleft G_{i+1} \Rightarrow g G_i g^{-1} = G_i$$

$$\rightarrow |\text{Stab}_{G_i}(x_j)| = |\text{Stab}_{g G_{i-1} g^{-1}}(x_k)| = |\text{Stab}_{G_i}(x_k)|$$

Allo $|B_j| = |B_k| \quad \forall j, k \rightarrow p = t \cdot |B_1| \rightarrow |B_1| \in \{1, p\}$

$\bullet |B_1| = 1 \rightarrow |B_i| = 1 \quad \forall i \Rightarrow G_i = \text{def} \rightarrow i=n$

$\bullet i < n \Rightarrow |B_1| = p \quad \checkmark$

$$2. p \mid |G_i| \quad \forall i \leq n-1 \rightarrow |G_{n-1}| = p$$

$$\left| \frac{G_{n-1}}{G_n} \right| = q \text{ primo} \quad \text{e} \quad |G_n| = 1 \rightarrow p \nmid q \text{ primo } p \neq q$$

3. G_{n-1} è l'unico sgr di ordine p di G

$$G < S_p, \quad p^2 \nmid p! \Rightarrow p^2 \nmid |G| \Rightarrow p \nmid \left| \frac{G_{i+1}}{G_i} \right| \quad \forall i < n-1 \quad (*)$$

$$\text{Inoltre } |G| = \prod_{i=1}^{n-1} \left| \frac{G_{i+1}}{G_i} \right|$$

Se $H < G$ t.c. $|H| = p$: $H = G_0$, suppongo $H < G_i$

$$\begin{array}{c} \text{ordine } p \\ \underline{H} \end{array} \xrightarrow{\quad} G_i \xrightarrow{\quad} G_i / G_{i+1} \xrightarrow{(*)} \mathcal{C}(H) = \bar{e} \rightarrow H < G_{i+1}$$

$\searrow \quad \quad \quad \nearrow$
 $\mathcal{C}$

$$\rightarrow H < G_i \quad \forall i \text{ (induzione)} \Rightarrow H < G_{n-1} \xrightarrow{\text{ord } p} H = G_{n-1}$$

Prop: K campo, $f \in K[x]$ irriducibile, separabile, $\partial f = p$ primo
 $L = \text{Cds di } f/K$

$$\text{Gal}(L/K) \text{ risolubile} \Rightarrow \forall \alpha, \beta \text{ radici di } f: L = K(\alpha, \beta)$$

Dm: G transitivo in S_p + irriducibile $\Rightarrow G$ lineare $\rightarrow$ numero di $\neq$ id $\neq$ p fissano 2 radici
(irriducibile + p)

$$\rightarrow \forall \alpha, \beta \text{ radici di } f: K(\alpha, \beta) \subset L \text{ e fissato solo da id } \rightarrow K(\alpha, \beta) = L$$

Oss: f irriducibile su $\mathbb{Q}$ di grado primo:
se f ha almeno 2 radici reali ed almeno una non reale $\Rightarrow \text{Gal}(f/\mathbb{Q})$ non risolubile

$$\left(\begin{array}{l} \text{conjugie fisso le 2 radici reali} \rightarrow 2\text{-ciclo in } G \\ \text{una di grado } p \rightarrow p\text{-ciclo in } G \end{array} \rightarrow G \simeq S_p \right)$$

- A anello (comm con 1), G gruppo $\rightarrow A[G] = \{ \sum_{g \in G} a_g g \mid a_g \in A \}$
con operazioni

$$\sum a_g g + \sum b_h h = \sum_{g+h \in G} (a_g + b_h) (g+h)$$

$$\sum a_g g \sum b_h h = \sum_{gh \in G} (a_g b_h) (gh)$$

anello
anello di gruppo

M è un $A[G]$ -modulo: $\rho: A[G] \rightarrow \text{End}(M)$

$M|_A \Rightarrow M$ è un A -modulo

$M|_G \Rightarrow G \rightarrow \text{Aut}(M)$ omo

D'altra parte se M è un A -modulo e un G -insiem ($\exists \rho: G \rightarrow \text{Aut}(M)$)
 $\Rightarrow M$ è un $A[G]$ -modulo

In particolare se $\rho: G \rightarrow \text{Aut}(M)$ omo e M gruppo abeliano
 $\rightarrow M$ è uno $\mathbb{Z}[G]$ modulo

- Data L/k di Galois, $G = \text{Gal}(L/k)$ si ha che

- L è un k -spazio
- $G \curvearrowright L$ per automorfismo $\Rightarrow L$ è un $K[G]$ -modulo

* TEO [della Base Normale]

L/k di Galois finita, $G = \text{Gal}(L/k) = \langle \sigma_1, \dots, \sigma_n \rangle$

$\Rightarrow L$ è un $K[G]$ -modulo libero di rango 1

$\Leftrightarrow \begin{cases} \exists \alpha \in L \text{ t.c. } L = K[G]\alpha \\ \exists \alpha \in L \text{ t.c. } \{\sigma_i(\alpha), \dots, \sigma_n(\alpha)\} \text{ } k\text{-base di } L \end{cases}$

Oss: $k = \mathbb{Q}$ e L estensione finita di $\mathbb{Q}$: $\mathbb{Z} \hookrightarrow \mathcal{O}_L = \text{"interi di } \mathbb{Q}$ "
Se $L/\mathbb{Q}$ di Galois con gruppo G : $\mathcal{O}_L$ è $\mathbb{Z}[G]$ -modulo.
In generale non è libero.

Dim: Caso K campo finito (sostanzialmente algebro lineare)

L/k finita di campo finito: $\text{Gal}(L/k) = \langle \phi \rangle$ Frobenius, $K = \mathbb{F}_{p^n}$
e $\phi(x) = x^p$

$\Rightarrow [L:K] = n$ quindi poiché ϕ è K -lineare,
per char di $\phi \rightarrow P_\phi = x^n - 1$ ($\phi^n = \text{id}$ e il deg è giusto)

per mps di $\phi \rightarrow P_\phi \mid P_\phi^m$ ma $1, \phi, \dots, \phi^{n-1}$ sono linearmente
indipendenti per il teo di
indipendenza dei caratteri

$\rightarrow \deg P_\phi \geq n \rightarrow P_\phi = P_\phi^m$
di $\dim \leq n$

Lemma: V K -spazio e $\sigma: V \rightarrow V$ K -lineare con $P_\sigma = P_\sigma^m$.
 $\rightarrow V$ è un $K[x]$ -modulo ciclico via σ .
(equiv. $\exists \alpha \in V$ t.c. $\{\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)\}$ K -base di V)

Oss: il Lemma conclude la dim in questo caso:

$\rightarrow \{\alpha, \phi(\alpha), \dots, \phi^{n-1}(\alpha)\}$ è una K -base di L .

Dim (Lemma) V è un $K[x]$ -modulo via σ :
 $\alpha \cdot v \mapsto \sigma(\alpha)v$: $K[x] \xrightarrow{\sigma} \text{End}(V)$
 $f(x) \mapsto f(\sigma) : V \rightarrow V$

Perché $K[x]$ è un PID e V è finitamente generato come $K[x]$ -modulo (e in gen in $K \subset K[x]$)

$$\Rightarrow V \cong \frac{K[x]}{(p_1^{e_1})} \times \dots \times \frac{K[x]}{(p_r^{e_r})} \quad \boxed{x \in K[x]^+}$$

perché $\dim_K V < +\infty$

$$\Rightarrow \mu_\sigma = [p_1^{e_1}, \dots, p_r^{e_r}]$$

$$P_\sigma = \prod_{i=1}^r p_i^{e_i} = \prod_{i=1}^r [p_i^{e_i}] \rightarrow p_i \text{ sono a due a due coprimi}$$

$$\xrightarrow{\text{TCR}} V \cong K[x] / \prod_{i=1}^r p_i^{e_i} \cong K[x] / (P_\sigma) \quad (\alpha \leftrightarrow 1)$$

$\bar{x}$ un $K[x]$ -modulo ciclico generato da $\bar{x}$
 $\rightarrow \{1, \bar{x}, \dots, \bar{x}^{n-1}\}$ è una K -base.

Caso K campo infinito:

Prop1: L/K finite e separabile $\Rightarrow \text{Hom}_K(L, \bar{K}) = \{\alpha_1, \dots, \alpha_n\}$
 $n = [L:K]$

Allora dati $\{\alpha_1, \dots, \alpha_n\} \in L$
sono una base di L in $K \Leftrightarrow \text{disc}(\alpha_i) := |\sigma_i(\alpha_j)|^2 \neq 0$
det della matrice di Vandermonde

Oss: $\text{disc}(\alpha_1, \dots, \alpha_{n-1}) = \text{disc} \mu_\alpha = \prod_{i < j} (\alpha_i - \alpha_j)^2$
det della matrice di Vandermonde

Dim: $\{\alpha_1, \dots, \alpha_n\}$ linearmente dip in $K \Leftrightarrow \text{disc}(\alpha_1, \dots, \alpha_n) = 0$

Infatti $\{\alpha_i\}$ lin. dip $\Leftrightarrow \exists c_1, \dots, c_n: \sum c_i \alpha_i = 0$ (*)

Ma allora se $\sigma_i = \omega_i \rightarrow |\sigma_i(\alpha_j)|^2 = \left| \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \sigma_1 \alpha_1 & \sigma_1 \alpha_2 & \dots & \sigma_1 \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n \alpha_1 & \sigma_n \alpha_2 & \dots & \sigma_n \alpha_n \end{pmatrix} \right|^2$

Quindi

$$(*) \Leftrightarrow \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \sigma_1 \alpha_1 & \dots & \sigma_1 \alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n \alpha_1 & \dots & \sigma_n \alpha_n \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Leftrightarrow \det(\omega_i \alpha_j) = 0$$

Prop2: Sia K un campo infinito e L/K di Galois finite
 $G = \text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Allora:

$\alpha \in K$ è
finito NON
è vero
 $[L:K] = n$

$\rightarrow \forall f \in L[x_1, \dots, x_n] \neq 0 \exists \alpha \in L: f(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \neq 0$

Lemma: K campo, $S \subset K$ infinito. Allora $\forall f \in K[x_1, \dots, x_n] \neq 0$
esistono $s_1, \dots, s_n \in S$ t.c. $f(s_1, \dots, s_n) \neq 0$

Dim: Induzione su $n \geq 1$ (caso $n=1$, noto)

$f(x_1, \dots, x_n) = \sum f_i(x_1, \dots, x_{n-1}) x_n^i$ e per ip. ind.

esistono $s_1, \dots, s_{n-1} \in S$ t.c. $f(s_1, \dots, s_{n-1}, x) \neq 0$
(parte che non annulla un fd)

$\rightarrow \exists s \in S$ t.c. $f(s_1, \dots, s_{n-1}, s) \neq 0$.

$f(x_1, x_2)$
 $= x_1 - x_2^n$

$f(\alpha, \phi(\alpha), \dots, \phi^{n-1}(\alpha))$
 $= \alpha - \alpha = 0$
 $\forall \alpha$

Dim (Prop 2): $\alpha_1, \dots, \alpha_n$ K -base di L : per Prop 1: $\text{disc}(\alpha_1, \dots, \alpha_n) \neq 0$
 dove $A = (\sigma_i \alpha_j) \stackrel{H}{\parallel} A \parallel^2$

Considero:

$$K[x_1, \dots, x_n] \xrightarrow{\varphi} K[y_1, \dots, y_n]$$

$$x_i \mapsto \sum_j \sigma_i(\alpha_j) y_j$$

$$f(x_1, \dots, x_n) \mapsto g(y_1, \dots, y_n) = f \circ A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

cambio lineare di variabile attraverso
 la matrice A : φ è BIGETTIVA ($\det A \neq 0$)

$$\Rightarrow f(x_1, \dots, x_n) \mapsto g(y_1, \dots, y_n) \text{ e } \underline{f \neq 0 \Leftrightarrow g \neq 0}$$

Per il Lemma in g : $\exists s_1, \dots, s_n \in K$ t.c. $g(s_1, \dots, s_n) \neq 0$
 $\Rightarrow f(A \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}) \neq 0$ cioè

$$f\left(\sum \sigma_i(\alpha_j) s_j, \dots, \sum \sigma_n(\alpha_j) s_j\right) \neq 0$$

$$\text{e detto } \alpha := \sum \alpha_j s_j \rightarrow f(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \neq 0$$

Quindi: stiamo cercando $\alpha \in L$ t.c. $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$ sia una
 K -base di L
 e questo è equiv a richiedere che

$$\text{disc}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) = \left(\det((\sigma_i \alpha_j))\right)^2 \neq 0$$

Considero $\varphi: \{1, \dots, n\}^2 \rightarrow \{1, \dots, n\}$
 $(i, j) \mapsto K$ t.c. $\sigma_i \circ \sigma_j = \sigma_k$

e $\varphi(i, \cdot)$ è una permutazione: in ogni riga (e in ogni col) ho una permut. di $\{1, \dots, n\}$
 $(\sigma_i \circ \sigma_j = \sigma_k \Leftrightarrow j = k)$

(i) $\rightarrow$ In ogni riga e in ogni col σ_k compare esattamente 1 volta

Scegli $x_1, \dots, x_n$ indeterminate: $(X_{\varphi(i,j)})$ è una matrice

$$\text{e considero } d(x_1, \dots, x_n) = \left| (X_{\varphi(i,j)}) \right| \neq 0$$

$$d(1, 0, \dots, 0) = (-1)^{n-1} |I_{n \times n}|$$

infatti per (i) in ogni riga e ogni colonna compare esattamente una volta 1.

$\rightarrow$ In particolare

$$d(x_1, \dots, x_n) \neq 0 \xrightarrow{\text{Prop 2}} \exists \alpha \in L: d(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \neq 0$$

$$\text{Ma } d(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) = \left| (\sigma_i(\alpha)_{\varphi(i,j)}) \right|^2 = \text{disc}(\sigma_i(\alpha)) \neq 0$$

* COOMOLOGIA DI GALOIS A G-modulo

$\rightarrow AG = \{a \in A \mid ga = a \ \forall g \in G\} \subset A$ ed e G-modulo banale

A, B G-moduli: $f: A \rightarrow B$ è un G-omomorfismo se f è omo di gruppi e $f(ga) = g f(a)$

$\text{Hom}(A, B) = \{ \text{omo di gruppi} \}$ ammette una G-moduli ponendo struttura

$$(g \cdot f)(x) := g f(g^{-1}x) \in A \text{ perche } A \text{ è un G-modulo}$$

$\hookrightarrow$ definisce un'azione da G su $\text{Hom}(A, B)$

$$\Rightarrow \text{Hom}(A, B)^G = \underline{\text{Hom}_G(A, B)} \text{ omo di G-moduli}$$

• SUCCESSIONI ESATTE

(*) $\dots \rightarrow P_i \xrightarrow{f_i} P_{i+1} \xrightarrow{f_{i+1}} P_{i+2} \rightarrow \dots$ successione esatta di moduli (oggetti) e omo di moduli (morfismi)

(*) è ESATTA in P_i se $\text{Im } f_{i-1} = \text{ker } f_i$

$\rightarrow$ Prop: $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ esatta di G-moduli: allora

$$0 \rightarrow A^G \xrightarrow{\alpha_G} B^G \xrightarrow{\beta_G} C^G \text{ è esatta}$$

(Niente in generale non si conserva l'esattezza a dx)

Dim: D'ero veduto: α_G iniettivo e $\text{Im } \alpha_G = \text{ker } \beta_G$ e che tutto è ben definito

1. α_G, β_G ben definite: $\alpha_G(a) = \alpha(a)$ e $(a \in A^G) \rightarrow g \alpha(a) = \alpha(ga) = \alpha(a) \rightarrow \alpha(a) \in B^G$ (uguale β_G)

2. α_G iniettivo perché $\alpha_G = \alpha|_{A^G}$ e α iniettivo su ip

3. $\text{Im } \alpha_G = \text{ker } \beta_G: \beta_G(\alpha_G(a)) = \beta(\alpha(a)) = 0$ su ip $\rightarrow \text{ker } \beta_G \supset \text{Im } \alpha_G$

Sia $b \in \text{ker } \beta_G: \exists a \in A$ t.c. $\alpha(a) = b$

$$\rightarrow b = gb = g\alpha(a) = \alpha(ga) = \alpha(a) \ \forall g \in G: \alpha \text{ mett: } a \in A^G$$

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)} \text{ do } \begin{array}{l} 1\text{-cocchi: } Z^1(G, A) = \{f: G \rightarrow A \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\} \\ 1\text{-cobochi: } B^1(G, A) = \{f: G \rightarrow A \mid f(\sigma) = \sigma(a) - a\} \end{array} \quad 05/16$$

$$G \curvearrowright A \text{ banale} \rightarrow H^1(G, A) = \text{Hom}(G, A)$$

$$\bullet \sigma(a) = a \ \forall a \in A, \sigma \in G \rightarrow B^1(G, A) = \{0\} \rightarrow H^1 = Z^1 \subset \text{Hom}(G, A)$$

$$\bullet \begin{array}{l} f(\sigma\tau) = f(\sigma) + f(\tau) \\ f(\sigma) + \sigma f(\tau) = f(\sigma) + f(\tau) \end{array} \rightarrow \text{Hom}(G, A) \subset Z^1(G, A)$$

Prop: $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ esatta, allora

$$0 \rightarrow A^G \xrightarrow{\alpha_G} B^G \xrightarrow{\beta_G} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha^*} H^1(G, B) \xrightarrow{\beta^*} H^1(G, C) \quad (*)$$

e' esatta.

Dim: Abbiamo già visto l'esattezza in A^G e B^G .

- $c \in C^G$ voglio definire $\delta(c)$: $\exists b \in B$ t.c. $\beta(b) = c$
Inoltre per tale β vale $\beta(\sigma b - b) = \beta(\sigma b) - \beta(b)$
 $= \sigma \beta(b) - \beta(b) = \sigma c - c = 0$

$$\Rightarrow \sigma b - b \in \ker \beta = \text{Im } \alpha$$

$$\text{ovvero } \exists a \in A \text{ t.c. } \sigma b - b = \alpha(a)$$

(A meno di insiemi fissare $\alpha(A) \in A$ non dire) $\sigma b - b = a \in A$

$$\delta(c) := f_b + B_1(G, A) \text{ dove } f_b(\sigma) = \sigma b - b \in B^1(G, B)$$

1. $\delta(c)$ è ben definito

- non dipende dalla scelta di b : $\beta b' = \beta b$ ha
 $f_{b'} = \sigma b' - b'$, $f_b = \sigma b - b \rightarrow b' - b \in \ker \beta = \alpha(A) = A$

$$\Rightarrow f_{b'}(a) = \sigma(b+a') - b - a' = \sigma b - b + \underbrace{\sigma(a') - a'}_{\in B^1(G, A)}$$

- è un omomorfismo circolare

$$f_b(\sigma \tau) = \sigma \tau b - b = \sigma \tau b - \sigma b + \sigma b - b = f_b(\sigma) - \sigma f_b(\tau)$$

2. $(*)$ esatta in C^G : $\text{Im } \beta_G = \ker \delta$

$$\bullet \underline{b \in B^G}: \delta(\beta_G(b)) = \delta(\beta(b)) = [\underbrace{\sigma b - b}_{=0}] = [0]$$

- Sia $c \in \ker \delta$: $\delta(c) = 0$ ovvero $f_b(\sigma) = \sigma b - b \in B^1(G, A)$
 $\rightarrow \exists a$ t.c. $f_b(\sigma) = \sigma a - a$ cioè: $\sigma(a-b) = a-b \quad \forall \sigma \in G$
 $\Rightarrow b-a \in B^G$
e $\beta(b-a) = \beta(b) = c \in \text{Im } \beta_G$

$$\bullet f \in H^1(G, A): \alpha^*(f) = \alpha \circ f \rightarrow \text{reufiché...}$$

$$\bullet f \in H^1(G, B): \beta^*(f) = \beta \circ f \rightarrow \text{reufiché...}$$

Considero una qualsiasi risoluzione ~~proiettiva~~ ^{di $\mathbb{Z}$} $(G$ -modulo liberi) in G -moduli liberi. $\mathbb{Z}$ è finitamente generato

$$P: \dots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \xrightarrow{k=0} \mathbb{Z} \rightarrow 0 \text{ dove } P_i = \mathbb{Z}[G]\text{-moduli liberi}$$

Considero allora il complesso $\text{Hom}_G(P, A)$ con A G -modulo:

$$0 \rightarrow \text{Hom}_G(P_0, A) \xrightarrow{d_0} \text{Hom}_G(P_1, A) \xrightarrow{d_1} \dots$$

$$\Rightarrow H^q(k) = \frac{\ker d_q}{\text{Im } d_{q-1}} =: H^q(G, A) \quad \forall q \geq 0$$

$$\begin{aligned} H^0 &= A^G \\ H^1 &= \frac{Z^1(G, A)}{B^1(G, A)} \end{aligned}$$

$$\text{Da } 0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0 \Rightarrow 0 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C)$$

l'om. è che
coincide di tutto
con questo come

$$\rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow \dots$$

◦ Hilbert 90 $\rightarrow L/k$ di Galois finite e $G = \text{Gal}(L/k)$
 $\Rightarrow H^1(G, L^*) = 0$

es: $\langle \xi_n \rangle = U_n$, L/k finita di Galois e $G = \text{Gal}(L/k)$

$$0 \longrightarrow U_n \xrightarrow{\iota} L^* \xrightarrow{\alpha^n} L^{*n} \longrightarrow 0 \text{ e esatta}$$

$$\xi_n \mapsto \xi_n \mapsto \alpha^n$$

$\Rightarrow$ Conduito

$$0 \rightarrow U_n^G \rightarrow (L^*)^G \rightarrow (L^{*n})^G \rightarrow H^1(G, U_n) \rightarrow H^1(G, L^*) = 0$$

$$0 \rightarrow U_n \xrightarrow{\iota} L^* \xrightarrow{\alpha^n} L^{*n} \xrightarrow{\beta} \text{Hom}(G, U_n) \rightarrow 0$$

$\chi: \sigma \mapsto \frac{\sigma(\xi_n)}{\xi_n}$ dove $\beta = \chi$

* TEORIA DI KUMMER

È una teoria per la classificazione delle estensioni abeliane di esponente finito

Def: G gruppo di esponente n e $G^n = \{1\}$

Sia K t.c. $\xi_n \in K$ e consideriamo le EST. ABELIANE di ESPONENTE n .

$\forall c \in K$ conduito $K(\sqrt[n]{c})/K$ ciclica e di esponente n
 e $\text{deg} \leq n$

Dato $\Delta \subset K$: $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{c} \mid c \in \Delta) = \prod_{c \in \Delta} K(\sqrt[n]{c})$

Prop 1: $L = K(\sqrt[n]{\Delta}) \Rightarrow L/k$ è abeliana di esponente n (di Kummer)

Dim: $\text{Gal}(L/k) \xrightarrow{\rho} \prod_{c \in \Delta} \text{Gal}(K(\sqrt[n]{c})/K)$

$\sigma \mapsto (\sigma|_{K(\sqrt[n]{c})})$

ρ iettivo: $\rho(\sigma) = \text{id} \Leftrightarrow \sigma(\sqrt[n]{c}) = \sqrt[n]{c} \quad \forall c \in \Delta \rightarrow \sigma = \text{id}$

$\Rightarrow \text{Gal}(L/k) \leq$ mod di gruppi ciclici di esponente n
 $\rightarrow$ È ABELIANO CON ESPONENTE n

Prop 2: L/k ABELIANA di ESPONENTE $n \Rightarrow L = K(\sqrt[n]{\Delta})$
 dove $\Delta = L^{*n} \cap K^*$

Dim: $\Delta \subset K^*$ e $\sqrt[n]{\Delta} \subset L \rightarrow K(\sqrt[n]{\Delta}) \subset L$
 $\cdot L = \prod L'$ dove $L' \subset L$ e L'/k finita $\Rightarrow L'/k$ abeliana finita di esp n
 (perché L/k finita)

$\Rightarrow L' =$ composto di estensioni cicliche su K di esp n

$\rightarrow L = \prod_{L' \text{ ciclica}} L' \Rightarrow$ per le teorie di Kummer sulle estensioni cicliche $\exists c \in K$ t.c. $L' = K(\sqrt[n]{c})$

Scelto $\Delta = K^* \cap L^{*n}$: $L' \subset K(\sqrt[n]{\Delta}) \quad \forall L' \text{ ciclica}$
 $\Rightarrow L = \prod L' \subset K(\sqrt[n]{\Delta})$

Oss 1: $L = K(\sqrt[n]{a}) \Rightarrow$ per il lemma di Steinitz $\Delta' = L^{*n} \cap K^*$
 $\Rightarrow K^{*n} < \Delta' < K^*$ e $L = K(\sqrt[n]{\Delta'})$ ($\Delta < \Delta'$)

Oss 2: $L = K(\sqrt[n]{a})$ con $a \notin K^{*n}$ $\forall d|h \rightarrow L/K$ ciclo di deg n
 infatti $L^{*n} \cap K^* = \bigcup_{i=0}^{n-1} a^i K^{*n}$ dove $\supset$ è ovvio.

Sia $c \in L^{*n} \cap K^*$: $\gamma := \sqrt[n]{c} \in L^* \Rightarrow \gamma = \sum_{i=0}^{n-1} c_i \alpha^i$ dove $\alpha = \sqrt[n]{a}$

quindi $\begin{cases} p_\gamma(x) \mid x^n - c \in K[x] & p_\alpha(x) = x^n - a \\ G = \text{Gal}(L/K) = \langle \sigma \rangle : \begin{cases} \sigma(\alpha) = \zeta_n \alpha \\ \sigma(\gamma) = \zeta_n^j \gamma \end{cases} \end{cases}$

D'altra parte $\sum \zeta_n^j \gamma = \sigma(\gamma) = \sigma(\sum c_i \alpha^i) = \sum c_i \zeta_n^i \alpha^i$ ovvero

$$\sum \zeta_n^j c_i \alpha^i = \sum \zeta_n^i c_i \alpha^i \rightarrow \sum \zeta_n^j c_i = \sum \zeta_n^i c_i \quad \forall i$$

$\{1, \alpha, \dots, \alpha^{n-1}\}$ linearmente indipendenti
 quindi $i \neq j \rightarrow c_i = 0$

ovvero $\gamma = c_j \alpha^j \rightarrow c = c_j^n \alpha^j \in \alpha^j K^{*n}$

$\rightarrow L = K(\sqrt[n]{a}) \rightarrow L^{*n} \cap K^* = \langle a K^{*n} \rangle$
 cioè per il lemma $L = K(\sqrt[n]{\langle a K^{*n} \rangle})$

Oss 3: $K(\sqrt[n]{a}) = K(\sqrt[n]{b}) \Leftrightarrow \langle a K^{*n} \rangle = \langle b K^{*n} \rangle$
 $\Leftrightarrow \exists h$ con $(h, n) = 1$ t.c. $ab^h \in K^{*n}$
 (*)

Infatti: (*) $\Leftrightarrow K^*/K^{*n} : a^{-1} K^{*n} \in \langle b K^{*n} \rangle$
 $\Leftrightarrow a^{-1} K^{*n} = b^h K^{*n} \Rightarrow ab^h \in K^{*n}$
 $(h, n) = 1$

* TEOREMA [di Kummer]

char $K \nmid n$, $\exists n \in K$: le estensioni abeliane di esponente n di K
 sono in corrispondenza biunivoca con i
 sgr di K^* che contengono K^{*n}

Precisamente:

$$\begin{array}{ccc} \{L/K \text{ di esponente } n\} & \leftrightarrow & \{\Delta \mid K^{*n} < \Delta < K^*\} \\ L & \xrightarrow{\alpha} & L^{*n} \cap K^* \\ K(\sqrt[n]{\Delta}) & \xleftarrow{\beta} & \Delta \end{array}$$

Inoltre c'è un isomorfismo canonico: $\Delta/K^{*n} \xrightarrow{\psi} \text{Hom}_{\text{cont}}(\text{Gal } L/K, U_n)$
 dove $L = K(\sqrt[n]{\Delta})$
 $\alpha K^{*n} \mapsto \chi_\alpha \left(\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \right)$

Oss: questo teorema garantisce l'esistenza di una
 estensione di Kummer massima $\rightarrow K(\sqrt[n]{K^*})$

$$K(\sqrt[n]{K^*})$$

* CARATTERI DI UN GRUPPO ABELIANO FINITO

05/21

G gruppo abeliano: $\hat{G} = \text{Hom}(G, \mathbb{C}^*) \leftarrow$ gruppo dei caratteri di G

Se G ha esponente n , $\hat{G} = \text{Hom}(G, \mathbb{U}_n)$
 $\rightarrow$ radici n -esime dell'1

Lemma G abeliano finito $\Rightarrow G \cong \hat{\hat{G}}$

Dim: $G \cong \mathbb{Z}/m\mathbb{Z}$, $\hat{G} = \text{Hom}(G, \mathbb{C}^*) = \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$

$G = \bigoplus_{i=1}^k \mathbb{Z}/m_i\mathbb{Z}$, $\hat{G} = \text{Hom}(\bigoplus \mathbb{Z}/m_i\mathbb{Z}, \mathbb{C})$
 $\cong \bigoplus_{i=1}^k (\text{Hom}(\mathbb{Z}/m_i\mathbb{Z}, \mathbb{C})) \cong \bigoplus_{i=1}^k \mathbb{Z}/m_i\mathbb{Z}$

Lemma 2: G abeliano finito: $G \cong \hat{\hat{G}}$ canonicamente.

Dim: $G \rightarrow \hat{\hat{G}}$
 $g \mapsto \bar{g}: X \mapsto X(g)$

- omomorfismo: $((g+h)(X) = X(g+h) = X(g)X(h) = g(X)h(X))$

- iniettivo: $g: X \mapsto X(g) = 1 \quad \forall X \in \hat{G}$

$\rightarrow$ Sia $H = \langle g \rangle \triangleleft G \Rightarrow \forall X \in \hat{G} \Rightarrow \bar{X}: G/H \rightarrow \mathbb{C}^*$
 $H \subset \ker X$
 $\forall X \in \hat{G}$

Ma quindi: $\hat{G} \rightarrow \hat{G/H}$ $\bar{X} \mapsto X$ $\Rightarrow$ $|\hat{G}| \leq |\hat{G/H}|$
 $|\hat{G}| \leq |\hat{G/H}| \Leftrightarrow |H| = 1$

Ma quindi $\bar{X}$ è un isomorfismo (omo iniettivo fra gruppi con la stessa cardinalità)

Quindi possiamo accoppiare $G = \hat{\hat{G}}$

$\rightarrow$ Accoppiamento di dualità

$G \times \hat{G} \rightarrow \mathbb{U}_n$ $(g, X) \mapsto X(g)$ $\leftarrow$ bilineare e non degen.
 $\begin{cases} X(g) = 1 \quad \forall g \Leftrightarrow X = 1 \\ X(g) = 1 \quad \forall X \Leftrightarrow g = 1 \end{cases}$

$\rightarrow$ Dato un accoppiamento di dualità abbiamo la nozione di ortogonali

$H < G$: $H^\perp = \{ X \in \hat{G} \mid X(h) = 1 \quad \forall h \in H \}$

$= \{ X \in \hat{G} \mid H \subset \ker X \} < \hat{G}$

$X < \hat{G}$: $X^\perp = \{ g \in G \mid X(g) = 1 \quad \forall X \in X \}$

$= \{ g \in G \mid h \in \ker X \quad \forall X \in X \} = \bigcap_{X \in X} \ker X$

Prop: Valgono i seguenti fatti (dato G gruppo ab. f. n. t.)

1) $H^\perp \cong (\hat{G/H})$

2) $(H^\perp)^\perp = H$

Dim: $|H^\perp| = |\{ \chi \in \hat{G} \mid H \subseteq \ker \chi \}| \longrightarrow (\hat{G}/H) \text{ è m.e.t.v.}$

$\begin{array}{ccc} \chi & \xrightarrow{H} & \bar{\chi} \\ & \uparrow & \\ & H \in \ker \chi & \end{array}$
 $\bar{\chi}: G/H \rightarrow \mathbb{C}^*$

$$\Rightarrow H^\perp \hookrightarrow (\hat{G}/H)$$

Viceversa data $\bar{\chi}: G/H \rightarrow \mathbb{C}^*$ si solleva in modo unico a $G \rightarrow \mathbb{C}^*$ $\rightarrow$ è anche nullo in H $\rightarrow$ morfismo.

$$2) (H^\perp)^\perp = \bigcap_{\chi \in H^\perp} \ker \chi \supset H$$

$\uparrow$ $H^\perp = \{ \chi \mid H \subseteq \ker \chi \}$

Inoltre:

$$|H| \cdot |H^\perp| = |H| \cdot |\hat{G}/H| = |H| \cdot |G/H| = |G|$$

Sia $X = H^\perp$, allora $|X| |X^\perp| = |X| |\hat{G}/X| = |X| |\hat{G}_X| = |\hat{G}| = |G|$

$\Rightarrow |H| |X| = |X| |X^\perp| \rightarrow |H| = |X^\perp| = |(H^\perp)^\perp|$

Abbiamo: $\{H \leq G\} \longleftrightarrow \{X \leq \hat{G}\}$

$\begin{array}{ccc} H & \xleftrightarrow{\quad} & H^\perp \\ X^\perp & \xleftrightarrow{\quad} & X \end{array}$

Cor: è biviaria $(H \mapsto H^\perp \mapsto (H^\perp)^\perp = X + \text{cardinalità})$

ex: $\mathbb{Q}(\zeta_m): G = \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ in questo caso i caratteri si chiamano CARATTERI DI DIRICHLET

• Sia L/K di Galois abeliana finita con $G = \text{Gal}(L/K)$ abbiamo:

$$\{X \mid X \leq \hat{G}\} \longleftrightarrow \{H \mid H \leq G\} \longleftrightarrow \{F \mid K \subseteq F \subseteq L\}$$

$\begin{array}{ccccc} H^\perp & \longleftrightarrow & H & \longleftrightarrow & L^H \\ \downarrow \text{SL} & & & & \uparrow \\ (\hat{G}/H) & & & & \\ \downarrow \hat{} & & & & \\ \text{Gal}(\hat{L^H}/K) & \dashrightarrow & & & \end{array}$

TEO[Kummer] Le estensioni abeliane di esponente n di K sono in corrispondenza biunivoca con i sgr di K^* che contengono K^{*n}

(*) Inoltre c'è un iso canonico: $\Delta/K^{*n} \xrightarrow{\bar{\delta}} \text{Hom}_{\text{cont}}(\text{Gal}(K(\sqrt[n]{\Delta})/K), U_n)$

Dim: L/K di Kummer di esp n , $G = \text{Gal}(L/K)$ $\rightarrow L = K(\sqrt[n]{\Delta})$

$\text{Gal}(\hat{K(\sqrt[n]{\Delta})}/K)$

Dimostriamo primo (*). Sappiamo dalla teoria coomologica che esiste

$$\begin{array}{ccc} \delta: \Delta & \longrightarrow & \text{Hom}_{\text{cont}}(G, U_n) \\ a & \longmapsto & \chi_a \left(\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \right) \end{array}$$

1. f è ben definita: χ_a è omomorfismo continuo per la continuità basta osservare che

$$\begin{aligned} \chi_a^{-1}(1) &= \{ \sigma \in \text{Gal}(L/k) \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \} \text{ aperto} \\ &= \text{Gal}(L/k(\sqrt[n]{a})) \end{aligned}$$

in G .

$\text{min } K(\sqrt[n]{a})/K \text{ finita e } \downarrow \text{Gal}$

2. f omomorfismo continuo

3. f induce $\bar{f}$ del Test:

CASO L/k FINITA

$$0 \rightarrow U_n \rightarrow L^* \rightarrow L^{*n} \rightarrow 0 \text{ esatta}$$

da cui ottegniamo $\parallel 0 \rightarrow U_n \rightarrow K^* \xrightarrow{\eta} L^{*n} \cap K^* \xrightarrow{\delta} \text{Hom}(G, U_n) \rightarrow 0$

$a \mapsto \chi_a \sqrt[n]{a}$

ESATTA

$\Rightarrow f$ è surgettiva

$\bullet \ker f = \text{Im}(\eta) = K^{*n}$

$\Rightarrow \text{Hom}(G, U_n) \cong \Delta / K^{*n}$

CASO L/k INFINITA

$$\begin{aligned} \ker f &= \{ a \in \Delta \mid \chi_a(\sigma) = 1 \ \forall \sigma \in G \} \\ &= \{ a \in \Delta \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \ \forall \sigma \in G \} \\ &= \{ a \in \Delta \mid \sqrt[n]{a} \in K^* \} = K^{*n} \end{aligned}$$

Dimostriamo che f è surgettiva.

Sia $\{ \Delta_i \}_{i \in I}$ i.e. I insieme dei stig. di Δ tali che Δ_i / K^{*n} è finito

$\Rightarrow \{ L_i \}_{i \in I}$ sono tutte le sottoestensioni finite di L/k

$K \subset F \subset L$ allora $\leftarrow$

$F = K(\sqrt[n]{F^{*n} \cap K^*})$

$\Rightarrow \Delta_0 / K^{*n} \cong \text{Hom}(\text{Gal}(F/k), U_n)$

$\{ \text{citt. rapp. di } \Delta_i / K^{*n} \}$

$\rightarrow \{ \text{Gal}(L/L_i) \}_{i \in I} \leftarrow$ base di intorni di $G = \text{Gal}(L/k)$

e sia $\chi \in \text{Hom}_{\text{cont}}(G, U_n)$ $\ker \chi = \chi^{-1}(1)$ aperto in G

$\Rightarrow \exists$ i.t.c. $\text{Gal}(L/L_i) \subset \ker \chi$

Ma qui vol. χ passa al quoziente. $\bar{\chi}: \frac{\text{Gal}(L/k)}{\text{Gal}(L/L_i)} \cong \text{Gal}(L_i/k) \rightarrow U_n$

$\Rightarrow \bar{\chi} \in \text{Hom}(\text{Gal}(L_i/k), U_n) \cong \Delta_i / K^{*n} \exists a \in \Delta_i: \bar{\chi} = \chi_a$

Ma allora: $\chi(\sigma) = \bar{\chi}(\sigma|_{L_i}) = \sigma \frac{\sqrt[n]{a}}{\sqrt[n]{a}} \rightarrow \boxed{\chi = \chi_a}$

Vediamo adesso la corrispondenza biunivoca $L \xrightarrow{\alpha} L^{*n} \cap K^*$
 $\Delta \xrightarrow{\beta} K(\sqrt[n]{\Delta})$

La buona def l'abbiamo già verificata.

$$\bullet (\beta \circ \alpha) L = \beta(L^{*n} \cap K^*) = K(\sqrt[n]{L^{*n} \cap K^*}) = L$$

$$\bullet (\alpha \circ \beta) \Delta = \alpha(K(\sqrt[n]{\Delta})) = L^{*n} \cap K^* = \Delta'$$

Prop della scorsio 10.6.

So che $\Delta \subset \Delta'$: $\Delta \subset K^* \cap (K(\sqrt[n]{\Delta}))^{*n}$
 e inoltre per ipotesi ho che $K^{*n} \subset \Delta \subset K^*$

Inoltre poiché $\Delta' = L^{*n} \cap K^*$: $\Delta' / K^{*n} \cong \text{Hom}_{\text{cont}}(\text{Gal}(L/K), U_n)$

Se $\Delta \subsetneq \Delta' \Rightarrow \Delta / K^{*n} < \Delta' / K^{*n} \rightarrow \Delta / K^{*n} \cong X$ stare proprio ch Hom(-)

In particolare $X = \{ \chi_a \mid a \in \Delta \}$

CASO L/K FINITA $X < \text{Hom}(\text{Gal}(L/K), U_n)$

$$\text{Allora } H = X^\perp = \{ \sigma \in \text{Gal}(L/K) \mid \chi_a(\sigma) = 1 \ \forall a \in \Delta \}$$

$$= \{ \sigma \in \text{Gal}(L/K) \mid \sigma \sqrt[n]{a} = \sqrt[n]{a} \} = \{ 1 \}$$

$$\text{perch\'e } L = K(\sqrt[n]{\Delta}) \rightarrow |X^\perp| \cdot |X| = |\hat{G}| \rightarrow |X| = |\hat{G}|$$

$$\Rightarrow X = \hat{G} \text{ ma quindi } \Delta / K^{*n} = \Delta' / K^{*n}$$

CASO L/K INFINITA $\Delta = \bigcup_{i \in I} \Delta_i$ $\Delta_i \rightarrow L_i = K(\sqrt[n]{\Delta_i})$

e per ogni Δ so che $\Delta_i = \Delta_i' = L_i^{*n} \cap K^*$

$$\Rightarrow L = K(\sqrt[n]{\Delta}) = \bigcup_{i \in I} K(\sqrt[n]{\Delta_i}) = \bigcup_{i \in I} L_i \Rightarrow L^{*n} = \bigcup_{i \in I} L_i^{*n}$$

$\supset \text{ovv}$
 $\subset x \in L \rightarrow x \in L_i$
per qualche i

$$\text{Allora: } \Delta' = L^{*n} \cap K^* = \left(\bigcup_{i \in I} L_i^{*n} \right) \cap K^* = \bigcup_{i \in I} (L_i^{*n} \cap K^*) = \bigcup_{i \in I} \Delta_i' = \Delta$$

$\supset \text{ovv}$
 $\subset x^n \in L^{*n}$
 $\Rightarrow x \in L$ per qualche i

es : K con $\text{char } K \neq 2$: $K(\sqrt[n]{a}) = K(\sqrt[n]{b}) \Leftrightarrow a/b \in K^{*2}$

KUMMER : $(\Rightarrow) a K^{*2} = b K^{*2}$

K con $\text{char } K \neq n$, $\exists n \in K$: $K(\sqrt[n]{a}) = K(\sqrt[n]{b}) \Leftrightarrow \langle \bar{a} \rangle = \langle \bar{b} \rangle$

• f monico + separabile di grado n , $K[x]$: cds di f in L
 $\alpha_1, \dots, \alpha_n$ radici di $f \rightarrow G_f = \text{Gal}(K/L) \ni \{\alpha_1, \dots, \alpha_n\}$

Prop: le orbite di $\alpha_1, \dots, \alpha_n$ sotto l'azione di G_f $\longleftrightarrow$ fattori irriducibili di f in L
 "comparazioni"

Dim: $\mathcal{O}_1, \dots, \mathcal{O}_r$ orbite: allora $\forall i$

$f_i(x) = \prod_{\alpha \in \mathcal{O}_i} (x - \alpha)$ è irriducibile: $G_f \curvearrowright \mathcal{O}_i$ transitiva

- $\sigma f_i(x) = f_i(\sigma x) \quad \forall i: \text{for } \alpha \in \mathcal{O}_i \rightarrow \sigma \alpha \in \mathcal{O}_i$
 $\rightarrow f_i \in L[x]$

Oss: $G = \langle \sigma \rangle$: $\mathcal{O} = \{\text{cicli di } \sigma\}$

TEO: A UFD, $L = \text{Quot}(A)$ e $f \in A[x]$ monico. P primo di A

Allora: $\bar{f} \in A/P[x]$ e se $f \in \bar{f}$ non hanno radici multiple

$$\text{Gal}(L/P) = G_{\bar{f}}$$

$$\text{Gal}(\text{Quot}(A/P)/\text{Quot}(A/P)) = G_{\bar{f}} \rightarrow G_{\bar{f}} < G_f$$

(no dim)

ex: $f(x) = x^5 - x - 1 \in \mathbb{Z}[x]$

$$(\text{mod } 2): \bar{f}(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$$

$$(\text{mod } 5): \bar{f}(x) \text{ irriducibile (AS: mod } \mathbb{Z}/5\mathbb{Z} = \text{irriducibile})$$

$\Rightarrow f(x)$ è irriducibile e

$$G_{\bar{f}} \cong \langle (12 \cdot 5) \rangle = \langle \sigma \rangle < S_5$$

$$G_{\bar{f}} \cong \text{Gal}(\mathbb{F}_{25}/\mathbb{F}_5) = \langle (123)(45) \rangle = \langle \tau \rangle < S_5$$

$$\Rightarrow \langle \sigma \rangle < G_f, \langle \tau \rangle < G_f \text{ e } \tau^3 = (45) \in G_f: G_f = S_5$$

• K -algebre finite

A anello commutativo con moltiplicazione in K (campo), $\dim_K A < +\infty$

ex: L/K est di campi; $K[G]$; $L \times L$

L/K fin, M/K fin $\Rightarrow L \otimes_K M$ è una K -algebra finita

$$\text{es: } \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = (\mathbb{R}[x]/(x^2+1)) \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\uparrow} \mathbb{C}[x]/(x^2+1) \simeq \mathbb{C}^2$$

$$\frac{A[x]}{I} \otimes_A B \cong \frac{B[x]}{I}$$

• il div di 0 su $\overline{x+i}, \overline{x-i}$

$$\overline{x+i} = \overline{x} + \overline{i} = x \otimes 1 + 1 \otimes i = 1 \otimes 1 + 1 \otimes i$$

$$\underline{\text{es:}} \quad \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta) \simeq \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \left(\frac{\mathbb{Q}[x]}{(\mu_{\beta}(x))} \right) \simeq \frac{\mathbb{Q}(\alpha)[x]}{(\mu_{\beta}(x))}$$

- μ_{β} irreducibile su $\mathbb{Q}(\alpha) \rightarrow$ CAMPO
- altrimenti $\mu_{\beta} = \prod p_i \rightarrow \prod \frac{\mathbb{Q}(\alpha)[x]}{(\mu_{p_i}(x))} \simeq \prod \mathbb{Q}(\alpha, \beta_i)$

TEO DI STRUTTURA [della K -algebra finite]

Una K -algebra finita:

- Ha un # finito di ideali primi e sono tutti max: $m_1, \dots, m_n$ ($n \leq \dim_K A$)
- $\text{Jac}(A) = \bigcap_{i=1}^n M_i = \bigcap_{i=1}^n M_i = \text{Nil}(A)$ ed $\exists m: J^m = 0$
- $A \simeq \prod A/M_i$

[e un anello artimano]

Def: A K -alg finita si dice RIDOTTA se $\text{Nil}(A) = \text{Jac}(A) = 0$
LOCALE se $n=1$: $A \simeq A/M$

ex: gli exmp sopra sono di algebra ridotte

ex: $M = \frac{K[x]}{(\mu(x))}$: $L \otimes_K M \simeq \frac{L[x]}{(\mu(x))}$ non ha nilpotenti se μ separabile

$$\begin{matrix} L = \mathbb{F}_p(x) \\ K = \mathbb{F}_p(x^p) \end{matrix} : L = \frac{K[y]}{y^p - x^p} : L \otimes_K L = \frac{\mathbb{F}_p(x)[y]}{(y^p - x^p)} = \frac{L[y]}{(y-x)^p} \text{ LOCALE}$$

Teo: L/K finita: L/K sep $\Leftrightarrow L \otimes_K \bar{K}$ ridotta

L/K puri insepar $\Leftrightarrow L \otimes_K \bar{K}$ locale

$$\underline{\text{Dim:}} \quad \text{Hom}_K(L, \bar{K}) \simeq \text{Hom}_{\bar{K}}(L \otimes_K \bar{K}, \bar{K}) \simeq (*)$$

$$L \xrightarrow{f} \bar{K} \quad \mapsto \quad \phi(f \otimes 1) = f(1) \in \bar{K}$$

$$f(1) = \phi(f \otimes 1) \quad \hookrightarrow \quad \phi: L \otimes_K \bar{K} \rightarrow \bar{K}$$

$$\text{Sia } A = L \otimes_K \bar{K} \simeq \prod_{i=1}^r A/M_i \text{ e } A_{\text{rid}} = A/\text{Jac} A = \prod A/M_i$$

$$\underline{\text{oss:}} \quad \alpha \in \text{Nil}(A): \exists \phi: A \rightarrow \bar{K}, \phi(\alpha) = 0 \rightarrow \text{Jac} A \subset \ker \phi$$

$$(*) \simeq \text{Hom}_{\bar{K}}(A_{\text{rid}}, \bar{K})$$

$$\text{Inoltre } A_{\text{rid}} \simeq A/M_1 \times \dots \times A/M_r \simeq \bar{K}^r$$

$$\Rightarrow \dim_{\bar{K}} A_{\text{rid}} = r = [A_{\text{rid}} : \bar{K}]$$

A/M_i campo, $\bar{K}$ alg fin
 $\rightarrow A/M_i = \bar{K}$

$$\rightarrow |\text{Hom}_K(L, \bar{K})| = |\text{Hom}_{\bar{K}}(A, \bar{K})| = |\text{Hom}_{\bar{K}}(A_{\text{rid}}, \bar{K})| = r \leq [L : K]$$

$$L/K \text{ sep} \Leftrightarrow |\text{Hom}(L, \bar{K})| = [L : K] \Leftrightarrow \Rightarrow A_{\text{rid}} = A$$

$$[A_{\text{rid}} : \bar{K}] \leq [A : \bar{K}] = [L : K]$$

$$L/K \text{ puri insepar} \Leftrightarrow |\text{Hom}(L, \bar{K})| = 1 \Leftrightarrow \dim_{\bar{K}} A_{\text{rid}} = r = 1 \Leftrightarrow A \text{ locale}$$