Appunti di Teoria dei Campi e Teoria di Galois

Giacomo Mezzedimi

12 marzo 2016

Indice

Introduzione

Questi appunti nascono nel primo semestre dell'anno accademico 2015/2016, periodo nel quale io ho seguito il corso della professoressa Del Corso; seguono abbastanza fedelmente le lezioni tenute dalla professoressa, e i testi di riferimento sono i libri "Algebra" di Bosch, "Algebraic Number Theory" di Frohlich e Cassels (soprattutto per la parte di coomologia di gruppi di Galois), "Class Field Theory" di Neukirch e "Algebra" di Lang (questi ultimi due quasi esclusivamente per gli esercizi).
Gli esercizi presenti sono stati quasi tutti svolti in classe, e sono tutti contenuti nei testi citati sopra.
Avendo io stesso studiato su questi appunti, **dovrebbero** essere abbastanza sgombri da errori, ma chiedo a chiunque usi questi appunti di segnalarmi qualsiasi tipo di errore presente, ad esempio per mail (*mezzedimi@mail.dm.unipi.it*).
Questi appunti si trovano sulla mia pagina web *http://poisson.phc.unipi.it/~mezzedimi/*.

Giacomo Mezzedimi

1 Estensioni di campi

1.1 Estensioni finite e estensioni algebriche

Nel seguito sia L/K un'estensione di campi.

Definizione 1.1.1. L è un K-spazio vettoriale; definiamo **grado** dell'estensione $[L : K] = \dim_K(L)$.
Se $[L : K] < \infty$ l'estensione si dice **finita**, altrimenti si dice **infinita**.

Proposizione 1.1.1. *$K \subseteq F \subseteq L$. Se due fra L/F, F/K e L/K sono finite, allora lo è anche la terza. In particolare $[L : K] = [L : F] \cdot [F : K]$.*

Dimostrazione. Se $\{\omega_i\}_{i=1,\dots,m}$ è una F-base di L e $\{\alpha_j\}_{j=1,\dots,n}$ è una K-base di F, è facile vedere che $\{\omega_i\alpha_j\}_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ è una K-base di L. □

Definizione 1.1.2. $K \subseteq L$, $\alpha \in L$. α si dice **algebrico** su K se $\exists f(x) \in K[x]\backslash\{0\}$ tale che $f(\alpha) = 0$; altrimenti si dice **trascendente**.
L/K si dice **algebrico** se ogni $\alpha \in L$ è algebrico su K.

Osservazione. Sia L/K un'estensione e sia $\alpha \in L$. Consideriamo l'omomorfismo di anelli (surgettivo):

$$\begin{array}{rccc} \varphi_\alpha : & K[x] & \longrightarrow & K[\alpha] \\ & p(x) & \longmapsto & p(\alpha) \end{array}$$

Per definizione, si ha che $\mathrm{Ker}(\varphi_\alpha) \neq \{0\} \iff \alpha$ è algebrico; dunque, se α è trascendente, $\mathrm{Ker}(\varphi_\alpha) = \{0\}$ e perciò $K[x] \cong K[\alpha]$.
Se invece α è algebrico, allora $\mathrm{Ker}(\varphi_\alpha)$ è un ideale di $K[x]$, che è un PID, dunque $\mathrm{Ker}(\varphi_\alpha) = (\mu_\alpha(x))$ con $\mu_\alpha(x) \neq 0$.
Per il teorema di omomorfismo, la mappa di valutazione si quozienta a un isomorfismo:

$$\begin{array}{rccc} \overline{\varphi_\alpha} : & \frac{K[x]}{(\mu_\alpha(x))} & \xrightarrow{\sim} & K[\alpha] \\ & p(x) + (\mu_\alpha(x)) & \longmapsto & p(\alpha) \end{array}$$

Ma $K[\alpha] \subseteq L$ è un dominio, dunque $(\mu_\alpha(x))$ è primo, ma $K[x]$ è un PID, dunque $(\mu_\alpha(x))$ è massimale e di conseguenza $K[\alpha]$ è un campo; segue quindi che $K[\alpha]$ coincide con il suo campo delle frazioni $K(\alpha)$ e che $\mu_\alpha(x)$, scelto monico, è irriducibile.
Osserviamo infine che la K-base $\{\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}\}$ di $\frac{K[x]}{(\mu_\alpha(x))}$ va nella K-base $\{1, \alpha, \dots, \alpha^{n-1}\}$ di $K[\alpha]$.
Segue dunque:

Proposizione 1.1.2. *Sia $\alpha \in L$ algebrico su K. Allora $[K(\alpha) : K] = \deg(\mu_\alpha(x))$.*

Definizione 1.1.3. Secondo le notazioni dell'osservazione precedente, definiamo **polinomio minimo** di α il polinomio monico e irriducibile $\mu_\alpha(x)$.

Proposizione 1.1.3. *L/K finita $\Rightarrow$ L/K algebrica.*

Dimostrazione. Se $[L : K] = n$, allora $\forall \alpha \in L$, $1, \alpha, \dots, \alpha^n$ sono dipendenti su K e dunque esiste una relazione di dipendenza lineare fra di esse. □

Osservazione. Il viceversa è falso; fra poco esibiremo un controesempio.

Definizione 1.1.4. $\alpha_1, \ldots, \alpha_n \in L$. Allora definisco ricorsivamente $K(\alpha_1, \ldots, \alpha_n) := K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.
Se invece $S \subseteq L$ è un sottoinsieme, definisco:

$$K(S) := \bigcup_{\substack{S_f \subseteq S \\ S_f \text{ finito}}} K(S_f).$$

Osservazione. $K(S)$ è un campo, in quanto se $\alpha, \beta \in K(S)$, allora esistono $S_\alpha, S_\beta \subseteq S$ finiti tali che $\alpha \in K(S_\alpha)$ e $\beta \in K(S_\beta)$, e dunque $\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K(S_\alpha \cup S_\beta) \subseteq K(S)$ poiché $S_\alpha \cup S_\beta \subseteq S$ è finito.

Osservazione. $K(S)$ è il più piccolo sottocampo di L che contiene sia K sia S; in altre parole:

$$K(S) = \bigcap_{K, S \subseteq F \subseteq L} F.$$

Infatti l'inclusione $\supseteq$ è ovvia, in quanto $K(S)$ è un sottocampo di L che si va ad intersecare per ottenere $\bigcap_{K,S\subseteq F\subseteq L} F$, mentre per l'altra basta notare che $\forall K, S \subseteq F \subseteq L$ e $\forall S_f \subseteq S$ finito, $K(S_f) \subseteq F$ (poiché F è un campo), da cui $K(S) \subseteq F$ $\forall K, S \subseteq F \subseteq L$ e cioè $K(S) \subseteq \bigcap_{K,S\subseteq F\subseteq L} F$.

Definizione 1.1.5. $K, F \subseteq L$. Definisco il **composto** KF di K e F come il più piccolo sottocampo di L che contiene sia K sia E.

Osservazione. Per quanto visto, si ha che $KF = K(F) = F(K)$.

Proposizione 1.1.4. *$S \subseteq L$ sottoinsieme tale che ogni $\alpha \in S$ è algebrico su K. Allora $K(S)/K$ è algebrica. (Dunque L/K è algebrica $\iff$ è algebricamente generata).*

Dimostrazione. Sia $\gamma \in K(S)$; $\gamma \in K(\alpha_1, \ldots, \alpha_n)$ per certi $\alpha_1, \ldots, \alpha_n \in S$ per definizione.
Ma $K(\alpha_1, \ldots, \alpha_n)/K$ è finita (in quanto ogni $K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ è finita perché α_i è algebrico su K e a maggior ragione su $K(\alpha_1, \ldots, \alpha_{i-1})$), quindi algebrica, e perciò γ è algebrico su K. □

In realtà, con la dimostrazione precedente abbiamo anche mostrato:

Corollario 1.1.5. *Se L/K è finitamente generata da elementi algebrici, L/K è finita.*

Osservazione. Ogni campo K contiene o $\mathbb{Q}$ o $\mathbb{F}_p$ per un certo $p \in \mathbb{N}$ primo. Infatti, fissato K, consideriamo l'omomorfismo di caratteristica:

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \longrightarrow & K \\ & 1 & \longmapsto & 1_K \end{array}$$

Per il teorema di omomorfismo, $\frac{\mathbb{Z}}{\mathrm{Ker}(\varphi)} \hookrightarrow K$; se $\mathrm{Ker}(\varphi) = (0)$, allora $\mathbb{Z} \subseteq K$ e dunque $\mathbb{Q} \subseteq K$ (perché K è un campo) e $\mathrm{char}(K) = 0$; se invece $\mathrm{Ker}(\varphi) = p\mathbb{Z}$ (in quanto $\frac{\mathbb{Z}}{\mathrm{Ker}(\varphi)}$ è un dominio perché contenuto in un campo), si ha che $\mathbb{F}_p \subseteq K$ e $\mathrm{char}(K) = p$.

Esempio (Estensioni quadratiche). Sia L/K un'estensione di grado 2, con $\mathrm{char}(K) = \mathrm{char}(L) \neq 2$. Allora $L = K(\alpha)$ con α un qualunque elemento in $L - K$; se μ_α è il polinomio minimo di α, allora $L = K(\sqrt{\Delta})$, dove Δ è il discriminante del polinomio.
Dico che, se $a, b \in K^* - K^{*2}$, $K(\sqrt{a}) = K(\sqrt{b}) \iff ab \in K^{*2}$.

Dimostrazione. Vediamo l'implicazione $\Rightarrow$, (l'altra è del tutto ovvia).
$\sqrt{a} \in K(\sqrt{b}) \iff \sqrt{a} = x + y\sqrt{b} \iff a = x^2 + y^2 b + 2xy\sqrt{b} \Rightarrow 2xy = 0$ $(1, \sqrt{b})$ è una base di $K(\sqrt{b})) \Rightarrow xy = 0 \Rightarrow x = 0$ (altrimenti $a \in K^{*2}$) $\Rightarrow a = y^2 b \Rightarrow ab = y^2 b^2 \in K^{*2}$. □

Dunque le estensioni quadratiche di $K \not\supset \mathbb{F}_2$ sono parametrizzate da $\frac{K^*}{K^{*2}}$ tramite la mappa iniettiva:

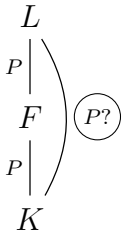
$$\begin{array}{ccc} \frac{K^*}{K^{*2}} & \longrightarrow & \{L \supseteq K | [L:K] = 2\} \\ aK^{*2} & \longmapsto & K(\sqrt{a}) \end{array}$$

<u>*Osservazione*</u>. L/K estensione. Allora $F = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$ è un'estensione algebrica di K.
Infatti è un campo in quanto se $\alpha, \beta \in F$, $\alpha, \beta \in K(\alpha, \beta)$ che è algebrico su K, quindi $\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K(\alpha, \beta) \subseteq F$, ed ovviamente F/K è algebrica.
Osserviamo inoltre che F è la più grande sottoestensione di L algebrica su K.

<u>*Esempio*</u> (Estensione algebrica non finita). Sia $F = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$. $F/\mathbb{Q}$ è algebrica ma non finita, in quanto $\forall n \in \mathbb{N}$, $\sqrt[n]{2} \in F$ e $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ (infatti $x^n - 2$ è irriducibile per il criterio di Eisenstein).

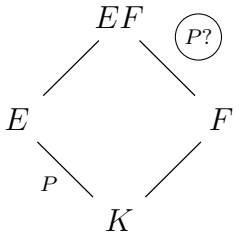
D'ora in poi, ogni volta che incontreremo una proprietà P sulle estensioni di campi, ci chiederemo se essa si conserva:

1. nelle torri di estensioni, cioè se P vale in L/F e F/K,



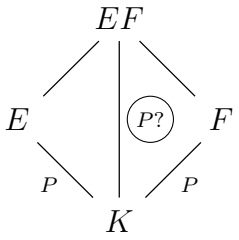
   è vero che P vale in L/K?

2. nel traslato, cioè se P vale in E/K,



   è vero che P vale in EF/F?

3. nel composto, cioè se P vale in E/K e F/K,



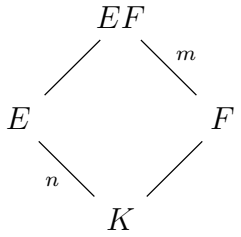
   è vero che P vale in EF/K?

<u>*Osservazione*</u>. Se la proprietà P si conserva nelle torri e nel traslato, allora è evidente che si conserva anche nel composto.

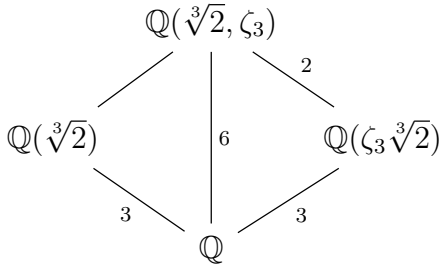
Vediamo ora se le proprietà "essere finita" e "essere algebrica" si conservano nei tre casi.

Proprietà. • P_1 = "essere finita".

1. P_1 si conserva nelle torri, come abbiamo già visto.
2. Per vedere che P_1 si conserva nel traslato, mostriamo che dato un diagramma:



allora $m \leq n$.
Questo segue dall'osservazione che, se $E = \langle w_1, \ldots, w_n \rangle_K$, allora $EF = \langle w_1, \ldots, w_n \rangle_F$ (ma in generale non si ha che $[EF : F] | [E : K]$; un controesempio può essere:



in quanto $2 \nmid 3$).

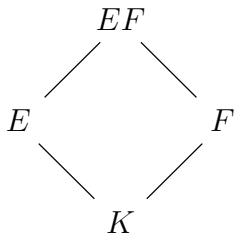
3. Visto che si conserva in 1 e 2, allora P_1 si conserva anche in 3.

- P_2 = "essere algebrica".

1. P_2 si conserva nelle torri; per vederlo consideriamo le estensioni:

e supponiamo che L/F e F/K siano algebriche. Sia $\alpha \in L$. Allora $\exists f(x) \in F[x] \backslash \{0\}$ tale che $f(\alpha) = 0$.
Se $f(x) = \sum_{i=0}^{n} a_i x^i$, α è algebrico su $F_0 = K(a_0, \ldots, a_n)$, ma $a_0, \ldots, a_n$ sono algebrici su K, quindi F_0/K è finita, ed essendo $F_0(\alpha)/F_0$ finita, si conclude che F_0/K è finita e dunque algebrica, cioè α è algebrico su K.

2. P_2 si conserva nel traslato; se abbiamo il diagramma:



e E/K è algebrica, allora $EF = F(E)/F$ è algebricamente generata, in quanto gli elementi di E sono algebrici su K e dunque su F, e quindi algebrica.

3. Visto che si conserva in 1 e 2, allora P_2 si conserva anche in 3.

1.2 Esistenza e unicità della chiusura algebrica

Definizione 1.2.1. F campo si dice **algebricamente chiuso** se soddisfa una delle seguenti condizioni equivalenti:

1. $\forall f(x) \in F[x]$, $\deg(f) \geq 1$, f ha una radice in F;
2. $\forall f(x) \in F[x]$, $\deg(f) \geq 1$, f si spezza completamente in F come prodotto di fattori lineari;
3. gli unici polinomi irriducibili di $F[x]$ sono quelli di grado 1.

Teorema 1.2.1 (fondamentale dell'algebra)**.** *$\mathbb{C}$ è algebricamente chiuso.*

Definizione 1.2.2. $K \subseteq F$. F si dice **chiusura algebrica** di K se è algebricamente chiuso e l'estensione F/K è algebrica.

Esempio. $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$ (è algebrica perché finita), ma non è la chiusura algebrica di $\mathbb{Q}$ (seguirà dal fatto che la chiusura algebrica di un campo infinito ha la stessa cardinalità del campo stesso).

Osservazione. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ è la chiusura algebrica di $\mathbb{Q}$.

Dimostrazione. Per quanto visto ci basta mostrare che $\overline{\mathbb{Q}}$ è algebricamente chiusa; sia dunque $f(x) \in \overline{\mathbb{Q}}[x] \subseteq \mathbb{C}[x]$ con $\deg(f) \geq 1$.
$\mathbb{C}$ è algebricamente chiuso, dunque $\exists \alpha \in \mathbb{C}$ tale che $f(\alpha) = 0$; α è algebrico su $\overline{\mathbb{Q}}$ che è algebrico su $\mathbb{Q}$, dunque α è algebrico su $\mathbb{Q}$ e cioè $\alpha \in \overline{\mathbb{Q}}$. □

Con la stessa dimostrazione si può mostrare:

Proposizione 1.2.2. *K campo e $L \supseteq K$ algebricamente chiuso. Allora $\overline{K} = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$ è una chiusura algebrica di K.*

In generale, dunque, il problema di trovare una chiusura algebrica per K si riduce a trovare un campo ambiente L, più grande di K, che sia algebricamente chiuso.

Lemma 1.2.3. *Siano $f_1(x), \ldots, f_n(x) \in K[x]$. Allora $\exists K' \supseteq K$ tale che f_i ha una radice in K' $\forall i = 1, \ldots, n$.*

Dimostrazione. Vediamolo per induzione su n:

$n = 1$) Se $f_1(x) = \mu_1^{e_1}(x) \cdot \ldots \cdot \mu_t^{e_t}(x)$ è la fattorizzazione di f_1 in $K[x]$, il campo

$$K' = \frac{K[x]}{(\mu_1(x))}$$

è tale che $\overline{x}$ è radice di f_1.

$n > 1$) Per ipotesi induttiva abbiamo $F \supseteq K$ in cui $f_1, \ldots, f_{n-1}$ hanno una radice. Come prima, se $f_n(x) = \gamma_1^{d_1}(x) \cdot \ldots \cdot \gamma_r^{d_r}(x)$ è la fattorizzazione di f_n in $F[x]$, si ha che

$$K' = \frac{F[x]}{(\gamma_1(x))}$$

è il campo voluto.

□

Teorema 1.2.4 (di esistenza di una chiusura algebrica)**.** *Sia K un campo. Allora $\exists \overline{K}$ chiusura algebrica di K.*

Dimostrazione. Come primo passo, cerchiamo un'estensione E_1 di K in cui ogni polinomio di $K[x]$ ha una radice.
Indicizziamo l'insieme $\{p(x) \in K[x] \mid \deg(P) \geq 1\} = \{p_\lambda(x)\}_{\lambda\in\Lambda}$; denotiamo dunque $X = \{x_\lambda\}_{\lambda\in\Lambda}$, dove x_λ è un'indeterminata "associata" al polinomio p_λ.
In $K[X]$ prendo l'ideale $I = (p_\lambda(x_\lambda))_{\lambda\in\Lambda}$ e affermo che $I \subsetneqq K[X]$.
Supponiamo per assurdo che si abbia

$$1 = \sum_{i=1}^{n} a_i p_{\lambda_i}(x_{\lambda_i})$$

per certi $a_1, \ldots, a_n \in K[X]$.
Sia $K' \supseteq K$ che contiene una radice α_i di $p_{\lambda_i}(x)$ $\forall i = 1, \ldots, n$ (che esiste per il lemma); consideriamo allora l'omomorfismo di valutazione:

$$\begin{array}{rccll} \varphi: & K[X] & \longrightarrow & K' & \\ & x_{\lambda_i} & \longmapsto & \alpha_i & \forall i = 1, \ldots, n \\ & x_\lambda & \longmapsto & 0 & \forall \lambda \in \Lambda \backslash \{\lambda_i\}_{i=1,\ldots,n} \\ & a & \longmapsto & a & \forall a \in K \end{array}$$

Abbiamo:

$$1 = \varphi(1) = \varphi\left(\sum_{i=1}^{n} a_i p_{\lambda_i}(x_{\lambda_i})\right) = \sum_{i=1}^{n} \varphi(a_i)\varphi\left(p_{\lambda_i}(x_{\lambda_i})\right) = \sum_{i=1}^{n} \varphi(a_i) p_{\lambda_i}(\alpha_i) = 0,$$

che è un assurdo.
Ma allora $I \subsetneqq K[X]$ e quindi $I \subseteq M$ ideale massimale. Definisco $E_1 = \frac{K[X]}{M}$.
Sicuramente $K \subseteq E_1$ (più precisamente $K \hookrightarrow E_1$), in quanto:

$$\psi : K \hookrightarrow K[X] \longrightarrow \frac{K[X]}{M} = E_1$$

e M non contiene 1, quindi ψ è iniettiva perché non nulla.
Preso ora E_1, ripetiamo il ragionamento appena concluso per ottenere E_2, e ricorsivamente costruiamo $K \subseteq E_1 \subseteq E_2 \subseteq \ldots$ in cui E_{i+1} contiene le radici dei polinomi di $E_i[x]$; definiamo:

$$E = \bigcup_{n\geq 1} E_n.$$

E è un campo perché unione di campi in catena. Dico che E è algebricamente chiuso.
Sia $f(x) \in E[x]$, $\deg(f) \geq 1$; $\exists j_0$ tale che $f(x) \in E_{j_0}[x]$, quindi in $E_{j_0+1} \subseteq E$ c'è una radice di f.
Concludo considerando $\overline{K} = \{\alpha \in E \mid \alpha \text{ è algebrico su } K\}$. □

<u>*Osservazione*</u>. Ripercorrendo la precedente dimostrazione, affermo che in realtà $\overline{K} = E$ (e dunque l'ultimo passaggio era inutile).
Per mostrarlo, basta vedere che E_i/E_{i-1} è algebrica $\forall i$ (basta vederlo su E_1/K, poiché per gli altri il ragionamento è analogo).
$E_1 = \frac{K[\{x_\lambda\}_{\lambda\in\Lambda}]}{M} = K\left[\{\overline{x_\lambda}\}_{\lambda\in\Lambda}\right]$, che è un'estensione di K algebricamente generata e dunque algebrica.

Esempio. Dico che

$$\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$$

è una chiusura algebrica di $\mathbb{F}_p$.

Dimostrazione. Sicuramente è un campo, poiché comunque dati $\mathbb{F}_{p^n}$ e $\mathbb{F}_{p^m}$, esiste $\mathbb{F}_{p^{nm}}$ che li contiene entrambi.
$\overline{\mathbb{F}_p}/\mathbb{F}_p$ è algebrica, poiché se $\alpha \in \overline{\mathbb{F}_p}$, $\alpha \in \mathbb{F}_{p^n}$ per un certo n e dunque α è algebrico su $\mathbb{F}_p$.
Infine, se $f(x) \in \overline{\mathbb{F}_p}[x]$, $\deg(f) \geq 1$, $\exists n$ tale che $f(x) \in \mathbb{F}_{p^n}[x]$; sicuramente $\exists \alpha$ in una chiusura algebrica di $\mathbb{F}_p$ tale che $f(\alpha) = 0$, ma allora $\mathbb{F}_{p^n}(\alpha) = \mathbb{F}_{p^{nd}}$ per un certo d, da cui f ha una radice in $\overline{\mathbb{F}_p}$. □

Osservazione. Sia K un campo infinito. Allora la cardinalità di una sua chiusura algebrica coincide con la cardinalità di K.

Dimostrazione. Denotiamo con A l'insieme degli elementi algebrici su K (in una chiusura algebrica).
Osserviamo innanzitutto che:

$$|K[x]| \leq \sum_{n\geq 0} |K[x]_{\leq n}| = \sum_{n\geq 0} |K|^{n+1} = \sum_{n\geq 0} |K| = \aleph_0 |K| = |K|,$$

in quanto $|K| = +\infty$.
Affermo che $|E_1| = |K|$ (e quindi ricorsivamente $|E_n| = |K|$ $\forall n$); si ha:

$$|E_1| \leq \sum_{\alpha \in A} |K(\alpha)| = |K| \cdot |A| \leq |K| \cdot |K[x]| = |K|^2 = |K|.$$

Si conclude notando che:

$$|E| = \sum_{n\geq 1} |E_n| = \aleph_0 |K| = |K|.$$

□

Richiamiamo ora una costruzione classica in teoria dei campi, la cosiddetta **estensione degli omomorfismi**.
Siano K,L campi, e sia $\varphi : K \hookrightarrow L$ un'immersione. Ci chiediamo per quali estensioni F/K algebriche esiste un $\widetilde{\varphi} : F \to L$ tale che $\widetilde{\varphi}_{|K} = \varphi$.

Osservazione. Il caso $F = K(\alpha)$, con α algebrico, è particolarmente semplice, in quanto dobbiamo definire solo $\widetilde{\varphi}(\alpha)$.
Sia μ il polinomio minimo di α su K. $\widetilde{\varphi}(\alpha)$ posso sceglierlo fra le radici di $\varphi(\mu)(x)$ in L, in quanto $\varphi(\mu)(\widetilde{\varphi}(\alpha)) = \widetilde{\varphi}(\mu(\alpha)) = 0$. Segue dunque:

Proposizione 1.2.5. *$F = K(\alpha)$ con α algebrico e $\varphi : K \hookrightarrow L$ immersione. Allora esistono esattamente m estensioni di φ a F dove $m = \#\{$radici distinte di $\varphi(\mu)$ in $L\}$.*
In particolare, se $\varphi = \mathrm{id}$ e $L = \overline{K}$, l'inclusione $i : K \hookrightarrow \overline{K}$ si estende a F in m modi, dove $m = \#\{$radici distinte di μ in $\overline{K}\}$.

Proposizione 1.2.6. *F/K algebrica. Se $\overline{K} \supseteq K$ é algebricamente chiusa, allora $\forall \varphi : K \hookrightarrow \overline{K}$, $\exists \psi : F \to \overline{K}$ tale che $\psi_{|K} = \varphi$.*

Dimostrazione. Sia $\mathcal{F} = \{(E, \psi) \mid K \subseteq E \subseteq F,\ \psi : E \to \overline{K} \text{ tale che } \psi_{|K} = \varphi\}$. Poniamo in $\mathcal{F}$ un ordine parziale definito da $(E, \psi) \preceq (E', \psi')$ se $E \subseteq E'$ e $\psi'_{|E} = \psi$.
$(\mathcal{F}, \psi)$ è induttiva: se $(E_\lambda, \psi_\lambda)_{\lambda\in\Lambda}$ è una catena, posto $E = \bigcup_{\lambda\in\Lambda} E_\lambda$ e $\psi : E \to \overline{K}$ tale che $\gamma \mapsto \psi_\lambda(\gamma)$ se $\gamma \in E_\lambda$ (e ψ è ben definita per la definizione di $\preceq$), allora (E, ψ) è un maggiorante della catena.
Per il lemma di Zorn, $\exists (F_0, \psi_0) \in \mathcal{F}$ massimale.
Dico che $F_0 = F$; se esistesse $\alpha \in F\backslash F_0$, $\psi : F_0 \to \overline{K}$ si estenderebbe a $\widetilde{\psi_0} : F_0(\alpha) \to \overline{K}$, assurdo per massimalità di F_0. □

Corollario 1.2.7 (Unicità della chiusura algebrica)**.** *Se $\overline{K}$ e $\overline{K}'$ sono chiusure algebriche di K, allora $\exists \psi : \overline{K} \to \overline{K}'$ isomorfismo tale che $\psi_{|K} = \mathrm{id}$.*

Dimostrazione. Sia $i : K \hookrightarrow \overline{K}$. $\overline{K}/K$ è algebrica, dunque per la precedente proposizione $\exists \psi : \overline{K} \to \overline{K}'$ tale che $\psi_{|K} = i$ (e dunque ψ è iniettiva perché non 0).
Resta da mostrare che ψ è surgettiva. Osserviamo che $\psi(\overline{K})$ è algebricamente chiuso; sia infatti $p(x) \in \psi(\overline{K})[x]$, cioè $p(x) = \psi(q)(x)$.
$q(x) \in \overline{K}[x]$, dunque $\exists \alpha \in \overline{K}$ tale che $q(\alpha) = 0$, da cui $p(\psi(\alpha)) = \psi(q)(\psi(\alpha)) = \psi(q(\alpha)) = 0$, cioè $\psi(\alpha) \in \psi(\overline{K})$ è una radice di p.
Visto che l'inclusione $\psi(\overline{K}) \subseteq \overline{K}'$ è ovvia, vediamo l'altra: sia $\gamma \in \overline{K}'$.
γ è algebrico su K, e a maggior ragione è algebrico su $\psi(\overline{K})$, quindi $\gamma \in \psi(\overline{K})$ perché $\psi(\overline{K})$ è algebricamente chiuso. □

Proposizione 1.2.8. *$K(\alpha)/K$ algebrica, $\mu_\alpha \in K[x]$ polinomio minimo di α, $\varphi : K \to \overline{K}$, $\deg \mu_\alpha = n$.*
Se μ_α ha m radici distinte in $\overline{K}$, allora φ si estende in m modi a $K(\alpha)$.

Dimostrazione. Sappiamo che $\#\{\text{estensioni di } \varphi \text{ a } K(\alpha)\} = \#\{\text{radici distinte di } \varphi(\mu_\alpha) \text{ in } \overline{K}\}$.
Vediamo che μ_α e $\varphi(\mu_\alpha)$ hanno lo stesso numero di radici in $\overline{K}$.
Siano $\{\alpha_1, \ldots, \alpha_m\} \subseteq \overline{K}$ le radici distinte di μ_α.

$$\mu_\alpha(x) = (x - \alpha_1)^{e_1} \cdot \ldots \cdot (x - \alpha_m)^{e_m}$$

fattorizzazione in $\overline{K}[x]$; sia $\widetilde{\varphi} : \overline{K} \to \overline{K}$ che estende φ. Allora:

$$\widetilde{\varphi}(\mu_\alpha)(x) = \varphi(\mu_\alpha)(x) = (x - \widetilde{\varphi}(\alpha_1))^{e_1} \cdot \ldots \cdot (x - \widetilde{\varphi}(\alpha_m))^{e_m},$$

e le $\widetilde{\varphi}(\alpha_i)$ sono distinte in quanto $\widetilde{\varphi}$, essendo non nulla, è iniettiva. □

<u>*Osservazione*</u>. Per il criterio della derivata, sui campi finiti e sui campi di caratteristica 0, i polinomi irriducibili hanno tutte radici distinte (in particolare, sui campi di caratteristica p, un polinomio ha una radice in comune con la sua derivata $\iff$ è somma di potenze p-esime $\iff$ è potenza p-esima.

<u>*Esempio.*</u> Sia $K = \mathbb{F}_p(t)$, $q(x) = x^p - t \in K[x]$ è irriducibile per il criterio di Eisenstein in $\overline{\mathbb{F}_p[t][x]}$ (che è un UFD), essendo t primo, ma quindi è irriducibile in $\mathbb{F}_p(t)[x]$ per il lemma di Gauss; inoltre $x^p - t = (x - \alpha)^p$ se α è una radice del polinomio in una chiusura algebrica, quindi q è un polinomio irriducibile con una sola radice.

1.3 Estensioni normali

Definizione 1.3.1. K campo, $f(x) \in K[x]$ con $\deg f \geq 1$. $L \supseteq K$ si dice **campo di spezzamento** di f su K se:

- $f(x)$ si spezza in fattori lineari in $L[x]$;

- L/K è generata dalle radici di f in L.

Osservazione. $\overline{K}$ chiusura algebrica di K fissata, $f \in K[x]$, $\deg f \geq 1$. Se $f(x) = (x-\alpha_1)^{e_1} \cdot \ldots \cdot (x-\alpha_n)^{e_n}$ in $\overline{K} \Rightarrow L = K(\alpha_1, \ldots, \alpha_n)$ è l'unico campo di spezzamento si f su K in $\overline{K}$.
Infatti $\overline{K}[x]$ è UFD, dunque a meno di permutazioni le radici di f in $\overline{K}$ sono $\alpha_1, \ldots, \alpha_n$.

Definizione 1.3.2. $\mathcal{F} = \{f_i\}_{i \in I}$, $f_i \in K[x]$, $\deg f_i \geq 1$ $\forall i$. L è un campo di spezzamento di $\mathcal{F}$ su K se:

- $\forall f_i \in \mathcal{F}$, f_i si spezza in fattori lineari in $L[x]$;
- L/K è generata dalle radici degli f_i in L.

Osservazione. Fissata una chiusura algebrica $\overline{K}$, L non è altro che $K\left[\{\alpha_{ij}\}_{i\in I}^{j=1,\ldots,n_i}\right]$, dove α_{ij} per $j = 1, \ldots, n_i$ sono le radici di f_i in $\overline{K}$.

Proposizione 1.3.1. *L, L' campi di spezzamento di $\mathcal{F}$ su K. Allora $\forall \sigma : L \to \overline{L'}$ tale che $\sigma_{|K} = \mathrm{id}$ si ha che $\sigma(L) = L'$.*

Dimostrazione. Vediamo innanzitutto il caso $\mathcal{F} = \{f\}$. $f(x) = c \cdot (x-\alpha_1)^{e_1} \cdot \ldots \cdot (x-\alpha_m)^{e_m}$ in L; inoltre $f(x) = \sigma(f)(x) = c \cdot (x-\sigma(\alpha_1))^{e_1} \cdot \ldots \cdot (x-\sigma(\alpha_m))^{e_m}$ in $\overline{L'}$, dunque per definizione $L' = K[\sigma(\alpha_1), \ldots, \sigma(\alpha_m)]$.
Nel caso generale si sfrutta il fatto che $L = \prod_{i\in I} L_i$ e si applica ripetutamente il caso precedente. □

Corollario 1.3.2. *L, L' campi di spezzamento di f su $K \Rightarrow L \cong L'$.*

Dimostrazione. Basta estendere $i : K \to \overline{L'}$ con la proposizione precedente. □

Definizione 1.3.3. Un'estensione F/K algebrica si dice **normale** se $\forall \varphi : F \to \overline{F}$ tale che $\varphi_{|K} = \mathrm{id}$ si ha $\varphi(F) = F$.

Proposizione 1.3.3. *F/K algebrica, $\varphi : F \to \overline{F}$ tale che $\varphi(F) \subseteq F$ e $\varphi_{|K} = \mathrm{id}$. Allora $\varphi(F) = F$.*

Dimostrazione. Se $[F : K] = n$, ho che $\dim_K \varphi(F) = \dim_K F$ e dunque $\varphi(F) = F$.
In generale, sia $\alpha \in F$; vediamo che $\alpha \in \varphi(F)$.
Sia μ_α il polinomio minimo di α su K; per ipotesi $\varphi(\mu_\alpha) = \mu_\alpha$, dunque per unicità della fattorizzazione φ, esteso a $\overline{F}$, agisce per permutazione sulle radici $\{\alpha_1, \ldots, \alpha_l\}$ di μ_α, cioè $\alpha \in \{\alpha_1, \ldots, \alpha_l\} = \{\varphi(\alpha_1), \ldots, \varphi(\alpha_l)\} \subseteq \varphi(F)$. □

Teorema 1.3.4. *F/K algebrica. Sono fatti equivalenti:*

1. *F/K è normale;*
2. *$\forall f \in K[x]$ irriducibile, vale che se f ha una radice in F, allora si spezza completamente in F;*
3. *F è il campo di spezzamento su K di una famiglia di polinomi di $K[x]$.*

Dimostrazione. $1 \Rightarrow 2)$ $f \in K[x]$ irriducibile, $f \sim \mu \in K[x]$ polinomio minimo delle sue radici (basta dividere per il leading coefficient), $\alpha \in F$ radice di μ. Presa β radice di μ e considerata l'immersione:

$$\begin{array}{rccc} \sigma : & K(\alpha) & \longrightarrow & \overline{F} \\ & \alpha & \longmapsto & \beta \end{array}$$

dell'identità su K, devo vedere che $\beta \in F$.
Sappiamo che $\exists \varphi : F \to \overline{F}$ tale che $\varphi_{|K(\alpha)} = \sigma$; sicuramente $\varphi(\alpha) = \beta$, ma $\varphi(F) = F$, dunque si ha che $\beta \in F$.

$2 \Rightarrow 3)$ Considero $I = \{\mu_\alpha\}_{\alpha \in F}$, dove μ_α è il polinomio minimo di α su K. Dico che F è il campo di spezzamento di I.
Sicuramente F è contenuto nel campo di spezzamento di I, ma per 2), μ_α ha tutte le radici in F, da cui la tesi.

$3 \Rightarrow 1)$ F campo di spezzamento di $\{p_i(x)\}_{i \in I}$; dunque $F = K\left(\{\alpha_{ij}\}_{i \in I}^{j=1,\dots,n_i}\right)$.
Sia $\varphi : F \to \overline{F}$ tale che $\varphi_{|K} = \mathrm{id}$. $\varphi(\alpha_{ij}) = \alpha_{ij'} \in F$, dunque $\varphi(F) = K(\{\varphi(\alpha_{ij})\}) \subseteq F$. □

Osservazione. Ogni estensione di grado 2 è normale, in quanto le radici sono coniugate.

Osservazione. Consideriamo la torre di estensioni $K \subseteq F \subseteq L$; se L/K è normale, allora L/F è anch'essa normale, in quanto soddisfa un'ipotesi più debole.

Esempi.
1. $\mathbb{Q}(\sqrt{p} \mid p \text{ primo})$ è normale su $\mathbb{Q}$, in quanto campo di spezzamento di $\{x^2 - p\}_{p \text{ primo}}$.
2. $\mathbb{Q}(\zeta_m \mid m \geq 2)$ è normale su $\mathbb{Q}$, in quanto campo di spezzamento dei polinomi ciclotomici su $\mathbb{Q}$.
3. $\mathbb{F}_p(\sqrt{a} \mid a \in \mathbb{F}_p) = \mathbb{F}_{p^2}$ se $p \neq 2$.
4. $\mathbb{F}_p(\zeta_m \mid m \geq 2) = \overline{\mathbb{F}_p}$.

Vediamo ora come si comportano le estensioni normali nelle torri, nel traslato e nel composto.

Proprietà. P_3 = "essere normale.

1. P_3 non si conserva nelle torri; in particolare, data la torre:

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

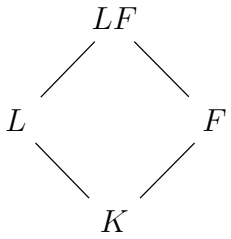
L/K normale $\not\Rightarrow$ F/K normale e un controesempio può essere:

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ \mathbb{Q} \end{array}$$

in quanto $\mathbb{Q}(\sqrt[3]{2})$ è reale ma $\mathbb{Q}(\zeta_3\sqrt[3]{2})$ non lo è.
Inoltre L/F normale e F/K normale $\not\Rightarrow$ L/K normale; un controesempio può essere:

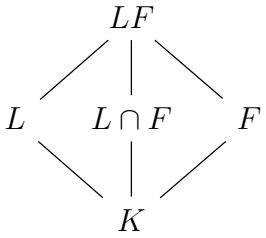
$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

2. P_3 si conserva nel traslato; consideriamo un diagramma:



Prendiamo $\psi : LF \to \overline{LF} = \overline{L}$ tale che $\psi_{|F} = \mathrm{id}$; $\psi(LF) = \psi(L)\psi(F)$, ma $\psi(F) = F$ e $\psi(L) = L$ per normalità di L/K (in quanto $\psi_{|K} = \mathrm{id}$).

3. P_3 si conserva nel composto; dato il diagramma:



se F/K e L/K sono normali, allora anche LF/K e $L \cap F/K$ lo sono. Per vederlo, prendiamo $\varphi : LF \to \overline{L}$ tale che $\varphi_{|K} = \mathrm{id}$. Allora $\varphi(LF) = \varphi(L)\varphi(F) = LF$ per normalità di entrambe; analogamente, se $\varphi : L \cap F \to \overline{L}$ è tale che $\varphi_{|K} = \mathrm{id}$, allora $\varphi(L \cap F) = \varphi(L) \cap \varphi(F) = L \cap F$.

Definizione 1.3.4. F/K algebrica, $\{\varphi_i\}_{i\in I}$ immersioni con $\varphi_i : F \to \overline{K}$. La **chiusura normale** di F/K è il campo $\widetilde{F} = \prod_{i\in I} \varphi_i(F)$.

Osservazione. Se $F = K(\alpha)$, con $\mu_\alpha(x) = (x-\alpha_1)^{e_1}\cdot\ldots\cdot(x-\alpha_m)^{e_m}$ in $\overline{K}$, allora $\widetilde{F} = \prod_i \varphi_i(F) = \prod_i K(\alpha_i)$ non è altro che il campo di spezzamento di μ_α.

Proposizione 1.3.5. *1. Fissata una chiusura algebrica $\overline{F}$ di F, $\widetilde{F}$ è la minima estensione normale di K che contiene F.*

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

Dimostrazione. 1. $\sigma : \widetilde{F} \to \overline{K}$ tale che $\sigma_{|K} = \mathrm{id}$; $\sigma(\varphi_i(F)) = (\sigma \circ \varphi_i)(F) = \varphi_j(F)$ per un certo $j \in I$, dunque $\widetilde{F}$ è normale su K.
Vediamo che è minima, cioè che se L/K è normale e $F \subseteq L$, allora $\widetilde{F} \subseteq L$.
Ogni $\varphi_i : F \to \overline{K}$ tale che $\varphi_{i|K} = \mathrm{id}$ si estende a $\widetilde{\varphi}_i : L \to \overline{K}$ tale che $\widetilde{\varphi}_i(L) = L$, dunque $\varphi_i(F) \subseteq \varphi_i(L) = L\ \forall i$ e perciò $\widetilde{F} = \prod F_i \subseteq L$.

2. Se $F = K(\alpha_1, \ldots, \alpha_n)$, $\widetilde{F}$ è campo di spezzamento su K di $\{\mu_{\alpha_1}, \ldots, \mu_{\alpha_n}\}$, dunque $\widetilde{F}/K$ è finita in quanto finitamente generata.

□

Definizione 1.3.5. F/K finita. Si definisce **nucleo normale** $\underline{F} = \bigcap_i \varphi_i(F)$.

Osservazione. Si può mostrare che è la massima sottoestensione di F/K normale su K.

Esercizio. *L/K normale, $f \in K[x]$ polinomio monico e irriducibile, $f = f_1 \cdot \ldots \cdot f_r$ in $L[x]$. Allora $\forall i, j\ \exists \sigma : L \to L$ con $\sigma_{|K} = \mathrm{id}$ tale che $\sigma(f_i) = f_j$.*

Dimostrazione. Sia α_i una radice di f_i e α_j una radice di f_j; α_i e α_j sono coniugate su K perché radici dello stesso polinomio minimo.
Se $\sigma : K(\alpha_i) \to \overline{K}$ con $\sigma_{|K} = \mathrm{id}$ realizza questo coniugio, cioè $\sigma(\alpha_i) = \alpha_j$, allora lo estendo a $\widetilde{\sigma} : L(\alpha_i) \to \overline{K}$ con $\widetilde{\sigma}_{|K(\alpha_i)} = \sigma$.
So che il polinomio minimo di α_i su L è f_i, dunque $\widetilde{\sigma}_{|L}(f_i)$ è il polinomio minimo di $\sigma(\alpha_i) = \alpha_j$, cioè $\widetilde{\sigma}_{|L}(f_i) = f_j$. □

1.4 Estensioni separabili

Definizione 1.4.1. $f \in K[x]\backslash\{0\}$, $\deg f \geq 1$ si dice **separabile** se le sue radici in $\overline{K}$ sono tutte distinte.

Osservazione. La definizione è ben posta, cioè non dipende dalla chiusura algebrica: se infatti $\overline{K}'$ è un'altra chiusura algebrica di K, esiste $\sigma : \overline{K} \to \overline{K}'$ che estende l'inclusione $i : K \to \overline{K}'$, dunque se $f(x) = (x-\alpha_1)^{e_1} \cdot \ldots \cdot (x-\alpha_m)^{e_m}$ in $\overline{K}[x]$, si ha che $\sigma(f)(x) = (x-\sigma(\alpha_1))^{e_1} \cdot \ldots \cdot (x-\sigma(\alpha_m))^{e_m}$ in $\overline{K}'[x]$ e le molteplicità non cambiano.

Proposizione 1.4.1 (Criterio della derivata)**.** *Sia $f \in K[x]\backslash\{0\}$, $\deg f \geq 1$. Allora:*

1. *f ha radici multiple (in una chiusura algebrica) $\iff$ $(f, f') \neq 1$ in $K[x]$;*
2. *se f è irriducibile, f ha radici multiple $\iff$ $f' = 0$.*

Dimostrazione.
1. Sia $\alpha \in \overline{K}$ una radice di f; $f(x) = (x-\alpha)g(x)$ per un certo $g(x) \in \overline{K}[x]$. Per la formula della derivata del prodotto, $f'(x) = g(x) + (x-\alpha)g'(x)$, per cui $f'(\alpha) = g(\alpha)$, dunque α è radice doppia $\iff$ $(x-\alpha) \mid (f, f')$ in $\overline{K}[x]$.
Ma se fosse che $(f, f') = 1$ in $K[x]$, si avrebbe che $a(x)f(x) + b(x)f'(x) = 1$ in $K[x]$ e dunque in $\overline{K}[x]$, assurdo.
2. Per 1), f ha radici multiple $\iff$ $(f, f') \neq 1$ in $K[x]$, ma $(f, f') \mid f$ che è irriducibile, dunque $(f, f') = f$. Ma $\deg f' < \deg f$, dunque $f' = 0$.

□

Corollario 1.4.2. *Sia $f \in K[x]\backslash\{0\}$ irriducibile, $\deg f \geq 1$. Allora:*

1. *se $\mathrm{char}(K) = 0$, f è separabile;*
2. *se $\mathrm{char}(K) = p$ e $r = \max\left\{k \in \mathbb{N} \;\middle|\; \exists g \in K[x] \text{ tale che } f = g\left(x^{p^k}\right)\right\}$, ogni radice di f ha molteplicità p^r, g è irriducibile in $K[x]$ e separabile e gli zeri di f sono le radici p^r-esime degli zeri di g.*

Dimostrazione.
1. Se $\mathrm{char}(K) = 0$, $\deg f' = \deg f - 1 \geq 0 \Rightarrow f' \neq 0$, dunque per la proposizione precedente f è separabile.
2. Innanzitutto tale r esiste, in quanto, se $S = \left\{k \in \mathbb{N} \;\middle|\; \exists g \in K[x] \text{ tale che } f = g\left(x^{p^k}\right)\right\}$, $0 \in S$ e $k \in S \Rightarrow \deg f \geq p^k$, dunque S è limitato e dunque ammette massimo.
Sia $g(x) = a_0 + \ldots + a_n x^n$; allora $f(x) = a_0 + \ldots + a_n x^{np^r}$.
Se si avesse che $g'(x) = a_1 + 2a_2 x + \ldots + na_n x^{n-1} = 0$, allora $ka_k = 0\ \forall k$, cioè $p \mid k$ o $p \mid a_k$, dunque si avrebbe che $g(x) = \sum_j a_{pj} x^{pj} = h(x^p)$ con $h(x) = \sum_j a_{pj} x^j$, da cui $f(x) = h\left(x^{p^{r+1}}\right)$, assurdo per massimalità di r.
Dunque g è separabile; inoltre è irriducibile (altrimenti neanche f lo sarebbe), e dunque

ha radici semplici: scriviamo $g(x) = \prod_i (x - \alpha_i)$, $\alpha_i \neq \alpha_j \ \forall i \neq j$.
Ma allora:

$$f(x) = g\left(x^{p^r}\right) = \prod_i \left(x^{p^r} - \alpha_i\right) = \prod_i \left(x^{p^r} - \beta_i^{p^r}\right) = \prod_i (x - \beta_i)^{p^r},$$

dove i β_i sono le radici p^r-esime degli α_i.

□

Definizione 1.4.2. L/K estensione di campi. $\alpha \in L$ algebrico su K si dice **separabile** su K se $\mu_\alpha(x)$ è separabile.
L/K si dice **separabile** se è algebrica e ogni $\alpha \in L$ è separabile su K.

Esempio. Se $K = \mathbb{F}_p(t)$ e $\alpha^p = t$, abbiamo visto che $K(\alpha)/K$ non è separabile.

Osservazione. Ogni campo di caratteristica 0 è tale che ogni sua estensione algebrica è separabile.

Definizione 1.4.3. K campo si dice **perfetto** se ogni sua estensione algebrica è separabile.

Osservazione. I campi di caratteristica 0 e i campi finiti sono perfetti (infatti in $\mathbb{F}_{p^n}$ un polinomio ha derivata $0 \iff$ è somma di potenze p-esime $\iff$ è una potenza p-esima).

Definizione 1.4.4. L/K algebrica. Definiamo **grado separabile** di L/K:

$$[L : K]_s = \left|\mathrm{Hom}_K(L, \overline{K})\right| = \#\left\{\varphi : L \to \overline{K} \;\middle|\; \varphi_{|K} = i : K \hookrightarrow \overline{K}\right\}.$$

Osservazione. Il numero $\left|\mathrm{Hom}_K(L, \overline{K})\right|$ è indipendente dalla chiusura algebrica: se $\overline{K}'$ è un'altra, detto $\sigma : \overline{K} \to \overline{K}'$ l'isomorfismo canonico fra di esse, è facile vedere che:

$$\begin{array}{ccc} \mathrm{Hom}_K(L, \overline{K}) & \longrightarrow & \mathrm{Hom}_K(L, \overline{K}') \\ \varphi & \longmapsto & \sigma \circ \varphi \end{array}$$

è una bigezione.

Osservazione. Se $\sigma : K \hookrightarrow \overline{K}$ è una qualsiasi immersione, allora:

$$\left|\mathrm{Hom}_K(L, \overline{K})\right| = \#\left\{\varphi : L \to \overline{K} \;\middle|\; \varphi_{|K} = \sigma\right\}$$

e una bigezione fra i due insiemi è data come prima da $\varphi \mapsto \widetilde{\sigma} \circ \varphi$, dove $\widetilde{\sigma} : \overline{K} \to \overline{K}$ è un'estensione di σ.

Proposizione 1.4.3. *$L = K(\alpha)$, α algebrico su K. Allora:*

1. $[K(\alpha) : K]_s = \#\{$*radici distinte di* μ_α *in* $\overline{K}\}$;
2. α *è separabile su* $K \iff [K(\alpha) : K]_s = [K(\alpha) : K]$;
3. *se* $\mathrm{char}(K) = p$ *e* p^r *è la molteplicità di* α *in* μ_α, *allora* $[L : K] = p^r[L : K]_s$.

Dimostrazione. I primi due punti seguono da fatti noti; vediamo il terzo.
Abbiamo visto che in questo caso $\mu_\alpha(x) = g\left(x^{p^r}\right)$, con $g \in K[x]$ irriducibile e separabile. Allora:

$$[L : K]_s = \#\{\text{radici distinte di } f\} = \#\{\text{radici distinte di } g\} = \deg g = \frac{\deg f}{p^r} = \frac{[L : K]}{p^r}.$$

□

Proposizione 1.4.4. *Il grado di separabilità è moltiplicativo nelle torri, cioè, date le estensioni $K \subseteq L \subseteq M$ con M/L e L/K algebriche e finite:*

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Dimostrazione. Sia $\overline{K}$ la chiusura algebrica di M. Poniamo $m = [M : L]_s = |\operatorname{Hom}_L(M, \overline{K})| = \#\{\tau_j\}$, $n = [L : K]_s = |\operatorname{Hom}_K(L, \overline{K})| = \#\{\sigma_i\}$; se $\widetilde{\sigma_i} : \overline{K} \to \overline{K}$ è un'estensione di σ_i, affermo che $\operatorname{Hom}_K(M, \overline{K}) = \{\widetilde{\sigma_i} \circ \tau_j\}$.
Sicuramente $\widetilde{\sigma_i} \circ \tau_j \in \operatorname{Hom}_K(M, \overline{K})$, in quanto se $a \in K$, $(\widetilde{\sigma_i} \circ \tau_j)(a) = \widetilde{\sigma_i}(\tau_j(a)) = \widetilde{\sigma_i}(a) = \sigma_i(a) = a$; inoltre se $\widetilde{\sigma_i} \circ \tau_j = \widetilde{\sigma_{i'}} \circ \tau_{j'}$, $\tau_j = \widetilde{\sigma_i}^{-1} \circ \widetilde{\sigma_{i'}} \circ \tau_{j'}$ e dunque $\forall b \in L$:

$$b = \tau_j(b) = (\widetilde{\sigma_i}^{-1} \circ \widetilde{\sigma_{i'}} \circ \tau_{j'})(b) = (\widetilde{\sigma_i}^{-1} \circ \widetilde{\sigma_{i'}})(b),$$

da cui $\widetilde{\sigma_i}(b) = \widetilde{\sigma_{i'}}(b)$, e cioè $\sigma_i = \sigma_{i'}$, da cui $i = i'$.
Di conseguenza, per invertibilità di $\widetilde{\sigma_i}$ e $\widetilde{\sigma_{i'}}$, si ha $\tau_j = \tau_{j'}$, cioè $j = j'$; dunque gli $\widetilde{\sigma_i} \circ \tau_j$ sono nm omomorfismi distinti.
D'altra parte, sia $\eta : M \to \overline{K}$ immersione che estende $i : K \hookrightarrow \overline{K}$; $\eta_{|L} \in \operatorname{Hom}_K(L, \overline{K})$, dunque $\eta_{|L} = \sigma_i$ per un certo i. Ora, per estendere σ_i a $\widetilde{\sigma_i}_{|M}$, per l'osservazione precedente ho esattamente $[M : L]_s = m$ possibilità, da cui $[M : K]_s \leq nm$. □

Proposizione 1.4.5. *L/K finita. Allora:*

1. *se* $\operatorname{char}(K) = 0$, $[L : K]_s = [L : K]$;
2. *se* $\operatorname{char}(K) = p$, *esiste* $r \in \mathbb{N}$ *tale che* $[L : K] = p^r [L : K]_s$.

Dimostrazione. Detta $L = K(\alpha_1, \ldots, \alpha_s)$, la tesi si ottiene usando la moltiplicatività del grado di separabilità nelle torri e le stesse relazioni mostrate per estensioni semplici. □

Proposizione 1.4.6. *L/K finita. Allora sono equivalenti:*

1. *L/K è separabile;*
2. *$\exists \alpha_1, \ldots, \alpha_s \in L$ separabili su K tali che $L = K(\alpha_1, \ldots, \alpha_s)$;*
3. *$[L : K] = [L : K]_s$.*

Dimostrazione. $1 \Rightarrow 2)$ $L = K(\alpha_1, \ldots, \alpha_s)$ e sicuramente tali elementi sono separabili.

$2 \Rightarrow 3)$ Essendo $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ separabile $\forall i$, la tesi segue applicando la moltiplicatività nelle torri del grado e del grado di separabilità e l'uguaglianza $[L : K] = [L : K]_s$ per le estensioni semplici.

$3 \Rightarrow 1)$ Sia $\alpha \in L$, $\mu_\alpha(x) \in K[x]$ il suo polinomio minimo; sicuramente $\exists p, r \in \mathbb{N}$ tale che $[K(\alpha) : K] = p^r [K(\alpha) : K]_s$, e α è separabile su $K \iff r = 0$.
Per ipotesi $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] = [L : K]_s = [L : K(\alpha)]_s \cdot [K(\alpha) : K]_s$, ma $[L : K(\alpha)]_s \mid [L : K(\alpha)]$ e $[K(\alpha) : K]_s \mid [K(\alpha) : K]$, dunque ci sono uguaglianze e quindi α è separabile su K.

□

Corollario 1.4.7. *L/K algebrica, $L = K(S)$ con $\emptyset \neq S \subseteq L$ sottoinsieme qualsiasi. Allora sono equivalenti:*

1. *L/K è separabile;*
2. *$\forall \alpha \in S$, α è separabile su K.*

Inoltre, se vale una delle due condizioni, si ha che $[L : K] = [L : K]_s$ *(possono anche essere infiniti).*

Dimostrazione. $1 \Rightarrow 2)$ Ovvia.

$2 \Rightarrow 1)$ Se $\alpha \in L$ e μ_α è il suo polinomio minimo su K, allora per definizione di $K(S)$ si ha che $\alpha \in K(\alpha_1, \dots, \alpha_m) = H$ per certi $\alpha_1, \dots, \alpha_m \in S$.
Ma H/K è finita e generata da elementi separabili, dunque per la proposizione precedente è separabile, da cui α è separabile su K.

Rimane da vedere che, se L/K è separabile e infinita, allora $[L : K]_s = +\infty$.
$\forall n \in \mathbb{N}$, esiste M_n tale che $K \subseteq M_n \subseteq L$ e $n < [M_n : K] < +\infty$, ma L/K è separabile, dunque M_n/K è separabile e quindi $[L : K]_s \geq [M_n : K]_s = [M_n : K] > n \ \forall n$, cioè $[L : K]_s = +\infty$. $\square$

<u>*Osservazione*</u>. Se $[L : K] = [L : K]_s = +\infty$, in generale non è vero che L/K è separabile.
Ad esempio, sia $K = \mathbb{F}_p(t)$ e $L = \overline{K}$; posto $F = \overline{\mathbb{F}_p}(t)$, sicuramente si ha che L/K non è separabile, ma è infinita (in quanto $[F : K] = +\infty$). Inoltre, $K \subsetneq F \subsetneq L$.
Ora F/K è separabile, in quanto $\overline{\mathbb{F}_p}(t) = \mathbb{F}_p(t)(\overline{\mathbb{F}_p})$ generato da elementi separabili, dunque $[F : K]_s = +\infty$ per la proposizione precedente; da questo concludiamo che $[L : K]_s \geq [F : K]_s = +\infty$.

Vediamo anche qua come si comporta la separabilità nelle torri, nel traslato e nel composto.

<u>*Proprietà*</u>. $P_4 =$ "essere separabile".

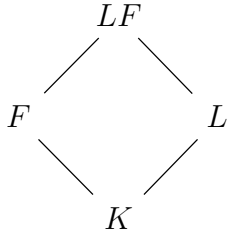
1. P_4 si conserva nelle torri; infatti, dato un diagramma:

   vale che L/K è separabile $\iff$ L/F è separabile e F/K è separabile.

   $\Rightarrow$) Sicuramente F/K è separabile in quanto $F \subseteq L$; inoltre il polinomio minimo di un elemento di L su F ha radici distinte perché è un divisore del polinomio minimo dello stesso elemento su K (che ha radici distinte per ipotesi).

   $\Leftarrow$) $\alpha \in L$; $\mu_\alpha \in F[x]$ polinomio minimo di α su F ha radici distinte. Se $a_1, \dots, a_n$ sono i coefficienti di μ_α, detto $F_0 = K(a_1, \dots, a_n)$, $K \subseteq F_0 \subseteq F_0(\alpha)$ e F_0/K è finita e separabile, e $F_0(\alpha)/F_0$ è finita e separabile, perché il suo polinomio minimo su F_0 divide il suo su F, da cui $F_0(\alpha)/K$ è finita e separabile e α è separabile su K.

2. P_4 si conserva nel traslato; consideriamo un diagramma:



   Se F/K è separabile, $LF = L(F)$, ma $\alpha \in F$ è separabile su $K \Rightarrow \alpha \in F$ è separabile su L, da cui LF/L è separabile in quanto separabilmente generata.

3. P_4 si conserva nel composto in quanto si conserva nelle torri e nel traslato.

Osservazione. Se L/K è separabile, allora la chiusura normale $\widetilde{L}/K$ è separabile. Infatti basta osservare che la separabilitá si conserva anche nel composto infinito, in quanto si conserva nel composto finito ed é una proprietá che dipende solo dagli elementi nel campo.

Definizione 1.4.5. L/K algebrica. Si definisce **chiusura separabile** di K in L il campo $K_s = \{\alpha \in L \mid \alpha \text{ è separabile su } K\}$.

Osservazione. K_s è effettivamente un campo, perché se $\alpha, \beta \in K_s$, allora $K(\alpha, \beta) \supseteq K(\alpha \pm \beta), K(\alpha\beta), K(\alpha^{-1}) \supseteq K$ e $K(\alpha, \beta)/K$ è separabile, cioè $\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K_s$.
Inoltre K_s è la massima sottoestensione di L/K separabile.

Teorema 1.4.8 (dell'elemento primitivo)**.** *Sia F/K un'estensione finita e separabile. Allora F è un'estensione semplice di K, cioè $\exists \gamma \in F$ tale che $F = K(\gamma)$.*

Dimostrazione. Se $|K| < +\infty$, allora $|F| < +\infty$, dunque F^* è ciclico, $F^* = \langle \xi \rangle$, da cui $F = K(\xi)$.
Sia invece $|K| = +\infty$; $F = K(\alpha_1, \dots, \alpha_n)$ per certi $\alpha_1, \dots, \alpha_n \in F$ separabili su K. A meno di una facile induzione, posso supporre $F = K(\alpha, \beta)$, α, β separabili su K.
$[F : K] = n \Rightarrow |\operatorname{Hom}_K(F, \overline{K})| = n$, quindi siano $\sigma_1, \dots, \sigma_n$ le immersioni di F/K. Cerco $\gamma \in F$ tale che $[F(\gamma) : F] = n$, cioè tale che $\deg \mu_\gamma = n$, cioè tale che $\sigma_1(\gamma), \dots, \sigma_n(\gamma)$ sono tutti distinti.
Sia x indeterminata; consideriamo l'elemento $\alpha + x\beta$ e il polinomio:

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

G ha $\binom{n}{2}$ fattori lineari, dunque ha grado $\leq \binom{n}{2}$; inoltre $G(x) \not\equiv 0$, poiché $\sigma_i(\alpha) + x\sigma_i(\beta) = \sigma_j(\alpha) + x\sigma_j(\beta) \iff \sigma_i(\alpha) = \sigma_j(\alpha)$ e $\sigma_i(\beta) = \sigma_j(\beta) \iff \sigma_i$ e σ_j coincidono su $F \iff i = j$.
Perciò G ha un numero finito di radici in $\overline{K}$.
Visto che K è infinito, $\exists t \in K$ tale che $G(t) \neq 0$, cioè $\sigma_i(\alpha) + t\sigma_i(\beta) \neq \sigma_j(\alpha) + t\sigma_j(\beta)\ \forall i \neq j$.
Se $\gamma = \alpha + t\beta$, si ha che $\sigma_i(\gamma) \neq \sigma_j(\gamma)\ \forall i \neq j$, come voluto. □

Teorema 1.4.9. *L/K finita. L/K è semplice $\iff |\{F \mid K \subseteq F \subseteq L\}| < +\infty$.*

Dimostrazione. Se $|K| < +\infty$, entrambe le condizioni sono sempre verificate, quindi il teorema vale.
Se $|K| = +\infty$, vediamo le due implicazioni:

$\Rightarrow$) Sia $L = K(\alpha)$. Denotiamo $\mu_{\alpha,F}$ il polinomio minimo di α su F; perciò $\mu_\alpha = \mu_{\alpha,K}$. Consideriamo la mappa:

$$\begin{array}{ccc} \{F \mid K \subseteq F \subseteq L\} & \longrightarrow & \{\text{divisori di } \mu_\alpha\} \\ F & \longmapsto & \mu_{\alpha,F} \end{array}$$

se mostro che è iniettiva ho la tesi.
Fissiamo $F \in \{F \mid K \subseteq F \subseteq L\}$; $\mu_{\alpha,F} \in F_0[x]$, dove $F_0 = K(a_1, \dots, a_n)$, con $a_1, \dots, a_n$ coefficienti di $\mu_{\alpha,F}$.
Visto che $F_0 \subseteq F$, sicuramente $\mu_{\alpha,F} \mid \mu_{\alpha,F_0}$, ma $\mu_{\alpha,F} \in F_0[x]$, quindi $\mu_{\alpha,F} = \mu_{\alpha,F_0}$.
A questo punto, se $\mu_{\alpha,F} = \mu_{\alpha,F'}$, allora $\mu_{\alpha,F} = \mu_{\alpha,F'} = \mu_{\alpha,F_0}$, da cui $F = F_0$ e $F' = F_0$, cioè $F = F'$.

$\Leftarrow$) A meno di un'induzione, posso supporre $L = K(\alpha, \beta)$.
Le estensioni $K(\alpha + t\beta)$ al variare di $t \in K$ sono infinite estensioni intermedie, dunque ne devono esistere due uguali, cioè $\exists t_1 \neq t_2 \in K$ tali che $K(\alpha + t_1\beta) = K(\alpha + t_2\beta)$.
$K(\alpha + t_1\beta) = K(\alpha + t_2\beta) \ni \beta(t_1 - t_2)$, ma $t_1 - t_2$ è invertibile, dunque $\beta \in K(\alpha + t_1\beta)$ e per differenza $\alpha \in K(\alpha + t_1\beta)$. Segue che $K(\alpha + t_1\beta) = K(\alpha, \beta) = L$.

□

Esempio (Estensione non semplice). Sia $L = \mathbb{F}_p(x, y)$ e $K = \mathbb{F}_p(x^p, y^p)$. K non è altro che $\phi(L)$, dove ϕ è il Frobenius di L. Dico che L/K non è semplice.
$K \subseteq K(x) \subseteq K(x)(y)$; si ha che $[K(x) : K] = p$, in quanto $[K(x) : K]_s = 1$ (poiché il polinomio $t^p - x^p$ ha un'unica radice in una chiusura algebrica), e dunque $[K(x) : K]$ deve essere una potenza di p (e quindi p perché x si annulla nel polinomio $t^p - x^p$); si deduce anche che $K(x) = \frac{K[t]}{(t^p - x^p)}$.
Analogamente si prova che $[K(x, y) : K(x)] = p$ e $K(x, y) = \frac{K(x)[t]}{(t^p - y^p)}$, da cui $[L : K] = p^2$, mentre $[L : K]_s = [L : K(x)]_s \cdot [K(x) : K]_s = 1$.
Mostro che ogni elemento di $L \backslash K$ ha grado p su K (e quindi l'estensione non può essere semplice). Sia $\alpha \in L \backslash K$.
$\alpha^p = \phi(\alpha) \in K$, dunque α è radice di $t^p - \alpha^p \in K[x]$ e perciò $[K(\alpha) : K] = p$.
Per il teorema precedente deduciamo che esistono infinite estensioni intermedie fra K e L.

Esercizio. *L/K estensione,* $\mathrm{char}(K) = p$*, $\alpha \in L$ algebrico su K. Allora α è separabile su $K \iff K(\alpha) = K(\alpha^p)$.*

Dimostrazione. $\Rightarrow$) $K(\alpha)/K$ è separabile; sia μ il polinomio minimo di α su $K(\alpha^p)$.
$K(\alpha)/K(\alpha^p)$ è separabile e $\mu \mid x^p - \alpha^p$, dunque $\mu = x - \alpha$ e $\alpha \in K(\alpha^p)$.

$\Leftarrow$) Se α non è separabile su K, $K[x] \ni \mu_\alpha(x) = g(x^{p^r})$ per un certo $r > 0$.
$\mu_{\alpha^p}(x) = g(x^{p^{r-1}})$, quindi $[K(\alpha^p) : K] = \deg \mu_{\alpha^p} \neq \deg \mu_\alpha = [K(\alpha) : K]$.

□

1.5 Estensioni puramente inseparabili

Osservazione. Sia K un campo e $\alpha \in \overline{K}$. Sappiamo che $\mu_\alpha(x) = g\left(x^{p^r}\right)$ per il massimo $r \geq 0$, dunque si ha la torre di estensioni:

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

in quanto sappiamo che $\mu_{\alpha^{p^r}}(x) = g(x)$ è separabile, dunque α^{p^r} è separabile su K, da cui:

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

Da questo si ricava anche che $K\left(\alpha^{p^r}\right)$ è la massima sottoestensione separabile di $K(\alpha)/K$.

Definizione 1.5.1. L/K finita. Definiamo **grado di inseparabilità** di L/K:

$$[L : K]_i = \frac{[L : K]}{[L : K]_s}.$$

Osservazioni.
- L/K finita è separabile $\iff [L:K] = [L:K]_s \iff [L:K]_i = 1$.
- Per quanto visto, se L/K è finita, allora $[L:K]_i = p^r$, con $p = \text{char}(K)$ e $r \geq 0$.
- Il grado di inseparabilità è moltiplicativo nelle torri, poiché lo sono sia il grado sia il grado di separabilità.

Definizione 1.5.2. $f \in K[x]$ si dice **puramente inseparabile** se ammette un'unica radice in $\overline{K}$.

Osservazioni.
- Se $\text{char}(K) = 0$, f è puramente inseparabile $\iff f = (x-a)^n$.
- Se $\text{char}(K) = p$, f è puramente inseparabile $\iff f = x^{p^r} - c$ (e f è irriducibile $\iff c$ non è potenza p-esima) o se $f = (x-a)^n$.

Definizione 1.5.3. $\alpha \in K$ si dice **puramente inseparabile** su K se $\mu_\alpha(x)$ è puramente inseparabile.
L/K si dice **puramente inseparabile** se ogni $\alpha \in L$ è puramente inseparabile su K.

Osservazioni.
- L/K puramente inseparabile $\Rightarrow L/K$ normale, in quanto il polinomio minimo di $\alpha \in L$ ha α come unica radice, e dunque L è campo di spezzamento di μ_α per tutti gli $\alpha \in L$.
- L/K separabile e puramente inseparabile $\Rightarrow$ è banale.
- $L = K(\alpha)$. α è puramente inseparabile su $K \iff [K(\alpha):K]_s = 1$ ($\iff [K(\alpha):K]_i = [K(\alpha):K]$).

Proposizione 1.5.1. *L/K algebrica. Allora sono fatti equivalenti:*

1. *L/K è puramente inseparabile;*
2. *$\exists S \subseteq L$ tale che $L = K(S)$ e $\forall \gamma \in S$, γ è puramente inseparabile su K;*
3. *$[L:K]_s = 1$;*
4. *$\forall \alpha \in L$, $\exists r \geq 0$ tale che $\alpha^{p^r} \in K$.*

Inoltre, se L/K è finita, ognuno di questi è equivalente a $[L:K] = [L:K]_i$.

Dimostrazione. $1 \Rightarrow 2)$ Ovvia perché $L = K(L)$.

$2 \Rightarrow 3)$ Ovvia, in quanto se $\sigma \in \text{Hom}_K(L, \overline{K})$, σ é l'identitá in quanto é l'identitá su un insieme di generatori.

$3 \Rightarrow 4)$ $\forall \alpha \in L$, $[K(\alpha):K]_s \mid [L:K]_s = 1$, quindi μ_α è puramente inseparabile su K, cioè $K[x] \ni \mu_\alpha(x) = x^{p^r} - \alpha^{p^r}$ per $p = \text{char}(K)$ e per un certo $r \geq 0$.

$4 \Rightarrow 1)$ Ovvia, perché se $\alpha \in L$, $\mu_\alpha(x) \mid x^{p^r} - \alpha^{p^r} \in K[x]$.

□

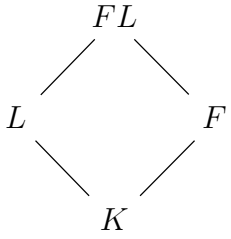
Come sempre, studiamo come si comportano le estensioni puramente inseparabili nelle classiche tre situazioni.

Proprietà. P_5 = "essere puramente inseparabile".

1. P_5 si conserva nelle torri, infatti per la proposizione precedente vale che, dato un diagramma:

   L/K è puramente inseparabile $\iff$ L/F è puramente inseparabile e F/K è puramente inseparabile (in quanto $[L:K]_s = 1 \iff [L:F]_s = 1$ e $[F:K]_s = 1$).

2. P_5 si conserva nel traslato, perché nella situazione:



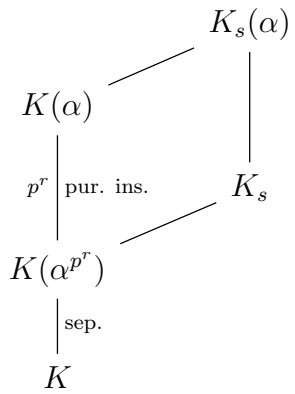
   se L/K è puramente inseparabile, lo è anche $FL = F(L)$ in quanto generata da elementi puramente inseparabili (su K e dunque) su F.

3. P_5 si conserva nel composto poiché si conserva sia nelle torri che nel traslato.

Abbiamo visto in un'osservazione che nel caso di un'estensione semplice, si può dividere la parte separabile da quella puramente inseparabile; il prossimo teorema ci assicura che questo può essere fatto in ogni caso.

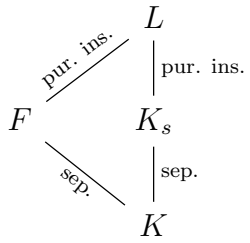
Teorema 1.5.2. *L/K algebrica, K_s chiusura separabile di L/K. Allora K_s/K è separabile, L/K_s è puramente inseparabile e K_s è univocamente determinato da queste proprietà.*
Inoltre si ha che $[L:K]_s = [K_s:K]$ e, se è definito, $[L:K]_i = [L:K_s]$.
Infine, se L/K è normale, allora K_s/K è normale.

Dimostrazione. Vediamo che L/K_s è puramente inseparabile; sia $\alpha \in L$. Si ha un diagramma:



in quanto $\alpha^{p^r} \in K_s$.
Ma $K(\alpha)/K(\alpha^{p^r})$ è puramente inseparabile, quindi lo è anche $K_s(\alpha)/K_s$, dunque α è puramente inseparabile su K_s.

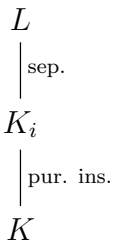
Vediamo ora che K_s è unico con tali proprietà: sia F sottoestensione di L/K tale che F/K è separabile e L/F è puramente inseparabile; abbiamo un diagramma:



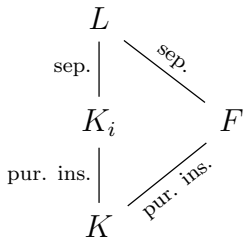
Ma F/K separabile $\Rightarrow F \subseteq K_s$, dunque K_s/F è separabile, ma $L \supseteq K_s \supseteq F$ e L/F è puramente inseparabile, da cui K_s/F è puramente inseparabile; segue che $F = K_s$.
Infine, se $\alpha \in K_s$, μ_α si spezza completamente in L, e ogni radice di μ_α è separabile su K perché lo è α, perciò le radici di μ_α stanno tutte in K_s. □

Ci chiediamo adesso se può essere costruita una sottoestensione di L/K che spezzi la parte separabile da quella puramente inseparabile al contrario, cioè che metta "sotto" la parte puramente inseparabile. Il seguente teorema ci dà una condizione sufficiente.

Teorema 1.5.3. *Sia L/K normale. Allora esiste un'unica sottoestensione K_i di L/K tale che:*



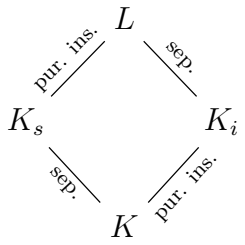
Dimostrazione. $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$ per normalità di L/K.
Pongo $K_i = L^{\mathrm{Aut}_K(L)} = \mathrm{Fix}(\mathrm{Aut}_K(L))$; con una banale verifica si vede che è un campo, e $K_i \supseteq K$.
K_i/K è puramente inseparabile, in quanto se $\varphi : K_i \to \overline{K}$ è tale che $\varphi_{|K} = \mathrm{id}$, lo estendo a $\widetilde{\varphi} \in \mathrm{Aut}_K(L)$, ma per definizione di K_i si ha che $\mathrm{id} = \widetilde{\varphi}_{|K_i} = \varphi_{|K_i} = \varphi$, cioè $[K_i : K]_s = 1$.
D'altra parte, K_i è la massima sottoestensione di L/K puramente inseparabile su K (poiché ogni estensione di questo tipo è fissata da $\mathrm{Aut}_K(L)$).
Vediamo inoltre che L/K_i è separabile; sia $\alpha \in L$. Consideriamo l'orbita (finita) di α sotto l'azione di $\mathrm{Aut}_K(L)$, $\mathrm{orb}(\alpha) = \{\sigma(\alpha)\}_{\sigma \in \mathrm{Aut}_K(L)} = \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$.
Sia $f(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha))$; $f(x) \in K_i[x]$, in quanto ogni automorfismo $\tau \in \mathrm{Aut}_K(L)$ agisce per permutazione su $\mathrm{orb}(\alpha)$, da cui $\tau(f) = f \ \forall \tau \in \mathrm{Aut}_K(L)$, perciò α è separabile su K_i perché radice di $f(x)$ separabile.
Infine vediamo che K_i è unico. Come nella dimostrazione precedente, abbiamo un diagramma:



F/K è puramente inseparabile, dunque $F \subseteq K_i$ e K_i/F è puramente inseparabile, ma $L \supseteq K_i \supseteq F$ e L/F è separabile, dunque K_i/F è separabile; combinando le due proprietà segue che $F = K_i$. □

É naturale ora la domanda se esista un'estensione L/K per cui non esiste un tale K_i. La risposta è affermativa, dunque facciamo qualche osservazione per capire in che modo costruire un esempio.

Osservazione. Supponiamo che si possa spezzare l'estensione L/K nei due modi:



Con il solito ragionamento, $K_i, K_s \subseteq K_iK_s \subseteq L$, ma L/K_s è puramente inseparabile e L/K_i è separabile, quindi $K_iK_s = L$.
Dunque, se è possibile questo doppio spezzamento con K_s/K normale, l'estensione $L = K_iK_s/K$ è normale in quanto composto di estensioni normali.
Quindi cerco un'estensione L/K non normale con tutte le sottoestensioni normali (in modo che, se esistesse K_i, si dovrebbe avere che L/K è normale, assurdo); ad esempio, se trovo un'estensione L/K non normale con $[L : K] = 4$ e $[L : K]_s = [L : K]_i = 2$, per quanto detto avrei l'esempio voluto.

Esempio. Sia $K = \mathbb{F}_2(x, y)$, $L = K(\alpha)$, dove α è radice di $\mu_\alpha(t) = t^4 + xt^2 + y = g(t^2)$; il polinomio è irriducibile perché di Eisenstein rispetto al primo $P = (x, y)$ e $[L : K]_s = [L : K]_i = 2$, in quanto $[L : K] = 4$ e il polinomio minimo di α si scrive come $g(t^2)$ (e dunque $[L : K]_i = 2$). Se vedo che L/K non è normale, ho finito.
$g(z) = z^2 + xz + y = (z - \gamma)(z - \delta)$ nella sua chiusura algebrica, quindi, se $\gamma = \alpha^2$ e $\delta = \beta^2$, nella chiusura algebrica si ha $\mu_\alpha(t) = (t - \alpha)^2(t - \beta)^2$.
Ovviamente, L/K è normale $\iff \beta \in L$. Sappiamo che $\alpha^2\beta^2 = y$ e $\alpha^2 + \beta^2 = (\alpha + \beta)^2 = x$, dunque $\alpha\beta = \sqrt{y}$ e $\alpha + \beta = \sqrt{x}$ (infatti la radice quadrata è unica in caratteristica 2).
Supponiamo per assurdo che $\beta \in L = K(\alpha)$. Allora $\sqrt{x}, \sqrt{y} \in L$ e dunque $K(\sqrt{x}, \sqrt{y}) \subseteq L$, ma $[K(\sqrt{x}) : K]_i = 2$ e $[K(\sqrt{x}, \sqrt{y}) : K(\sqrt{x})]_i = 2$, da cui $[K(\sqrt{x}, \sqrt{y}) : K]_i = 4$, assurdo.

1.6 Alcuni esercizi

Esercizio. *K di caratteristica p. Il Frobenius $\phi : K \to K$ è surgettivo $\iff$ K è perfetto.*

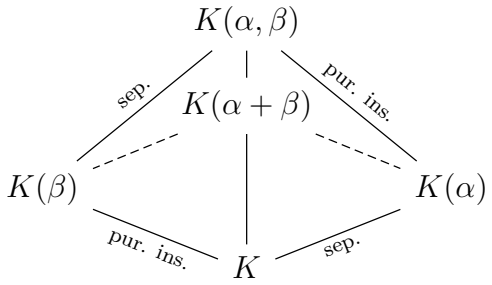
Dimostrazione. $\Rightarrow$) $\beta \in \overline{K}$. Vediamo che β è separabile su K.
Sicuramente $\mu_\beta(x) = g(x^{p^r}) \in K[x]$ per un certo $r \geq 0$, ma per surgettività di ϕ ho che $g(x^{p^r}) = h(x)^{p^r}$ per un certo $h(x) \in K[x]$, e dunque $r = 0$ per irriducibilità di μ_β.

$\Leftarrow$) Sia $b \in K$. $x^p - b \in K[x]$ e $x^p - b = (x - \beta)^p \in \overline{K}[x]$, ma $\beta \in \overline{K}$ è separabile su K, dunque $\mu_\beta(x) \in K[x]$ è separabile e $\mu_\beta(x) \mid (x - \beta)^p$, quindi $\mu_\beta(x) = x - \beta$ e cioè $\beta \in K$ (con $\beta^p = b$).

□

Esercizio. *L/K estensione, $0 \neq \alpha \in L$ separabile su K, $0 \neq \beta \in L$ puramente inseparabile su K. Allora $K(\alpha, \beta) = K(\alpha + \beta) = K(\alpha\beta)$.*

Dimostrazione. Abbiamo il diagramma:



dove le linee tratteggiate stanno ad indicare che vogliamo mostrare quelle inclusioni.
Siano $\sigma_1, \dots, \sigma_n$ le immersioni di $K(\alpha)/K$ (cioè $[K(\alpha,\beta) : K]_s = [K(\alpha) : K] = n$); estendiamo σ_i a $\widetilde{\sigma_i}$ immersione di $K(\alpha,\beta)/K$ tale che $\widetilde{\sigma_i}(\beta) = \beta$, cioè $\widetilde{\sigma_i}$ è un'immersione di $K(\alpha,\beta)/K(\beta)$.
Le $\widetilde{\sigma_i}$ sono tutte distinte su $K(\alpha+\beta)$, perché $\widetilde{\sigma_i}(\alpha+\beta) = \sigma_i(\alpha)+\beta = \sigma_j(\alpha)+\beta = \widetilde{\sigma_j}(\alpha+\beta) \iff \sigma_i(\alpha) = \sigma_j(\alpha) \iff i = j$, dunque $[K(\alpha+\beta) : K]_s = n$.
Ma allora $K(\alpha+\beta)$ contiene $K(\alpha)$ e dunque $\alpha, \beta \in K(\alpha+\beta)$, in quanto $\beta = (\alpha+\beta) - \alpha$.
Per $K(\alpha\beta)$ il ragionamento è del tutto analogo.
Osserviamo che l'esercizio poteva essere banalmente risolto osservando nel diagramma che $K(\alpha,\beta)/K(\alpha+\beta)$ è sia separabile che puramente inseparabile. □

Esercizio. *$L = K(\alpha,\beta)/K$ algebrica, α separabile su K. Allora l'estensione è semplice.*

Dimostrazione. Come nel teorema dell'elemento primitivo, $|K| = +\infty$. Posto $n = [L : K]_s = [K_s : K]$, consideriamo allo stesso modo il polinomio :

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

con σ_i immersioni di L/K; $F(x) \neq 0$, dunque $\exists 0 \neq t \in K$ tale che $F(t) \neq 0$.
Allora $[K(\alpha+t\beta) : K]_s = n$, perciò $K(\alpha+t\beta) \supseteq K_s \supseteq K(\alpha)$, da cui $\alpha \in K(\alpha+t\beta)$ e dunque $\beta \in K(\alpha+t\beta)$. □

Corollario 1.6.1. *Ogni estensione del tipo $K(\alpha_1, \dots, \alpha_n, \beta)$, con $\alpha_1, \dots, \alpha_n$ separabili, è semplice.*

Esercizio. *Sia K di caratteristica p. Denotiamo $K^{p^{-n}} := \{a \in \overline{K} \mid a^{p^n} \in K\}$; in pratica $K^{p^{-n}}$ non è altro il campo di spezzamento dei polinomi $\{x^{p^n} - c\}_{c \in K}$.*
Abbiamo dunque una catena $K \subseteq K^{p^{-1}} \subseteq K^{p^{-2}} \subseteq \dots$; definiamo $K^{p^{-\infty}} = \bigcup_{n\geq 1} K^{p^{-n}}$ ***chiusura perfetta*** *(o* ***chiusura puramente inseparabile****) di K. Allora:*

1. *$K^{p^{-\infty}}$ è perfetto;*
2. *K è perfetto $\iff K = K^{p^{-\infty}}$;*
3. *$[K^{p^{-\infty}} : K] = 1$ se K è perfetto e ∞ altrimenti.*

Dimostrazione.

1. Sia $a \in K^{p^{-\infty}}$; vediamo che è una potenza p-esima. $a \in K^{p^{-n}}$ per un certo n, dunque $x^{p^{n+1}} - a^{p^n} \in K[x]$; sia $b \in K^{p^{-n-1}}$ la radice di questo polinomio. Allora $(b^p)^{p^n} = a^{p^n}$, cioè $b^p = a$ e $b \in K^{p^{-n-1}} \subseteq K^{p^{-\infty}}$.

2. Vediamo l'implicazione $\Rightarrow$, essendo l'altra una banale conseguenza del primo punto.
Visto che il Frobenius è surgettivo, allora $K^{p^{-1}} = K$. Ma allora il Frobenius di $K^{p^{-1}}$ è surgettivo, dunque $K^{p^{-2}} = K^{p^{-1}}$. Iterando, si ha la tesi.

3. Supponiamo che $K^{p^{-\infty}} \supsetneqq K$, cioè che K non sia perfetto. Allora $\exists a \in K$ tale che $x^p - a$ è irriducibile su K (in quanto le radici di un polinomio puramente inseparabile hanno molteplicità potenza di p).
Dico che il polinomio $x^{p^n} - a$ è irriducibile $\forall n$. Infatti, se $x^{p^n} - a = (x-\alpha)^{p^n} \in \overline{K}[x]$ e per assurdo si avesse che $(x-\alpha)^{p^k} \in K[x]$ per $k < n$, allora $\left((x-\alpha)^{p^k}\right)^{p^{n-k}} = x^{p^n} - a$, e cioè $\alpha^{p^k} \in K$ sarebbe la radice p^{n-k}-esima di a, assurdo perché a non ha una radice p-esima in K.
Ma allora $[K^{p^{-\infty}} : K] \geq p^n \ \forall n$, cioè la tesi.

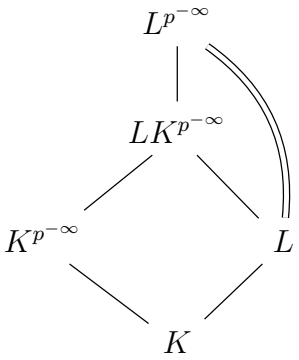
□

Esercizio. *L/K algebrica. Allora:*

1. *K perfetto $\Rightarrow$ L perfetto.*
2. *L perfetto e L/K finita $\Rightarrow$ K perfetto.*

Dimostrazione. 1. Se F/L è algebrica, allora F/K è algebrica, dunque separabile per perfezione di K, perciò F/L è separabile.

2. Abbiamo il diagramma:



in quanto $LK^{p^{-\infty}} \subseteq L^{p^{-\infty}}$ e $L = L^{p^{-\infty}}$ per perfezione di L.
Ma allora $K^{p^{-\infty}} \subseteq L$ e dunque $K^{p^{-\infty}}/K$ è finita, cioè $K = K^{p^{-\infty}}$.

□

Esercizio. *L/K algebrica e separabile. Sono fatti equivalenti:*

1. *$\forall f \in L[x]$ separabile, $\deg f \geq 1$, f si spezza completamente in $L[x]$;*
2. *Presa $\overline{K}$ chiusura algebrica di K che contiene L, allora $\overline{K}/L$ è puramente inseparabile.*

*Inoltre, dato K, $\exists L = \overline{K}_s$ algebrica e separabile su K tale che vale 1) o 2), e L è unica. Tale $\overline{K}_s$ prende il nome di **chiusura algebrica separabile** di K.*

Dimostrazione. $1 \Rightarrow 2)$ Sia $\alpha \in \overline{K}$ e sia $\mu_\alpha(x)$ il suo polinomio minimo su L; sicuramente $\mu_\alpha(x) = g(x^{p^r})$ per un certo $r \geq 0$. Ma allora α^{p^r} è separabile su L, e dunque il suo polinomio minimo $g(x)$ su L è separabile; perciò $g(x)$ ha grado 1, in quanto altrimenti per ipotesi non sarebbe irriducibile. Segue che $\alpha^{p^r} \in L$ e cioè che $\overline{K}/L$ è puramente inseparabile.

$2 \Rightarrow 1)$ Sia $f \in L[x]$, $\deg f \geq 1$, f irriducibile e separabile; vogliamo vedere che $\deg f = 1$.
Sia $\alpha \in \overline{K}$ una radice di f (in quanto $\overline{L}$ è una chiusura algebrica di K, che per unicità coincide con $\overline{K}$); allora $\alpha^{p^r} \in L$ per un certo $r \geq 0$, e dunque $f(x) \mid x^{p^r} - \alpha^{p^r}$, cioè $f(x) = x - \alpha$ per separabilità di f.
Osserviamo che il campo $\overline{K}_s$ appena costruito è la chiusura separabile di $\overline{K}/K$, che abbiamo visto essere unico con tali caratteristiche. □

Osservazione. Dopo aver notato che $\overline{K}/K$ è normale, segue che esiste un campo $\overline{K}_i$ tale che $\overline{K}/\overline{K}_i$ è separabile e $\overline{K}_i/K$ è puramente inseparabile; è inoltre ovvio che $\overline{K} = \overline{K}_s\overline{K}_i$.

Esercizio. *L/K algebrica tale che ogni polinomio irriducibile di $K[x]$ ha almeno una radice in L. Allora $L = \overline{K}$.*

Dimostrazione. Per l'osservazione precedente, $\overline{K} = \overline{K}_i\overline{K}_s$. Voglio vedere che $\overline{K}_s, \overline{K}_i \subseteq L$.
Sia $\alpha \in \overline{K}_s$, μ_α il suo polinomio minimo su K. Sia F il campo di spezzamento di μ_α su K; visto che μ_α è separabile, allora F/K è finita e separabile e dunque per il teorema dell'elemento primitivo $F = K(\beta)$.
$\mu_\beta(x) \in K[x]$ e $F = K(\beta_i)$ $\forall \beta_i$ radice di μ_β (in quanto F/K è normale), ma $\exists i$ tale che $\beta_i \in L$, quindi $F \subseteq L$ e perciò $\alpha \in L$.
Con questo abbiamo visto che $\overline{K}_s \subseteq L$, quindi se $\operatorname{char} K = 0$, concludo che $L = \overline{K}$.
Se invece $\operatorname{char} K = p$, dico che $\overline{K}_i \subseteq L$; sia $\alpha \in \overline{K}_i$.
$\mu_\alpha(x) = x^{p^r} - c \in K[x]$, ma L contiene una radice di μ_α, che ha α come unica radice, quindi $\alpha \in L$. □

2 Estensioni di Galois

2.1 Richiami e prime proprietà

Sia L/K normale. $\mathrm{Aut}_K(L) = G$ è un gruppo e $|G| = |\operatorname{Hom}_K(L, \overline{K})| = [L : K]_s$. Se inoltre L/K è anche separabile, l'estensione è detta **di Galois** e $|G| = [L : K]$.
G prende il nome di **gruppo di Galois** di L/K e si indica con $\mathrm{Gal}(L/K)$.

Proposizione 2.1.1. *L/K normale, $K \subseteq E \subseteq L$. Allora $\mathrm{Aut}_E(L) < \mathrm{Aut}_K(L)$.*
Inoltre, se anche E/K è normale, la mappa:

$$\begin{array}{ccc} \mathrm{Aut}_K(L) & \longrightarrow & \mathrm{Aut}_K(E) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}$$

è surgettiva.

Proposizione 2.1.2. *L campo, $G < \mathrm{Aut}(L)$. Allora:*

1. *$|G| < +\infty \Rightarrow L/L^G$ è di Galois finita e $G = \mathrm{Gal}(L/L^G)$.*
2. *$|G| = +\infty$ e L/L^G algebrica $\Rightarrow L/L^G$ è di Galois infinita e $G < \mathrm{Gal}(L/L^G)$.*

Dimostrazione. Sicuramente L^G è un campo. Sia $|G| < +\infty$ o L/L^G algebrica; vediamo che L/L^G è separabile.
$\forall \alpha \in L$, $G\alpha = \mathrm{orb}_G(\alpha) = \{\sigma(\alpha)\}_{\sigma \in G}$ è finita, perché $\sigma(\alpha)$ varia fra i coniugati di α; sia $G\alpha = \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$.
Se $f(x) = \prod_{i=1}^n (x - \sigma_i(\alpha)) \in L^G[x]$, f è separabile e $f(\alpha) = 0$, dunque α è separabile su L^G.
Inoltre L/L^G è normale, perché L è campo di spezzamento su L^G di tutti i $\mu_\alpha(x)$ al variare di $\alpha \in L$ (in quanto l'inclusione $\subseteq$ è chiara, mentre per l'altra basta notare che μ_α divide il polinomio f di prima, che ha tutte radici in L).
Supponiamo ora $|G| = n$; $\forall \alpha \in L$, $[L^G(\alpha) : L^G] \leq n$, perché $\mu_\alpha \mid f$. Sia $m = \max_{\alpha \in L} \{[L^G(\alpha) : L^G]\}$ e sia $\alpha_0 \in L$ che realizza tale grado.
Se per assurdo $\exists \beta \in L \backslash L^G(\alpha_0)$, allora $L^G(\alpha_0, \beta) = L^G(\gamma)$ per il teorema dell'elemento primitivo, ma $[L^G(\gamma) : L^G] \leq m$ implica che $\beta \in L^G(\alpha_0)$, assurdo.
Ora $G < \mathrm{Aut}_{L^G}(L) = \mathrm{Gal}(L/L^G)$, e $n = |G| \leq |\mathrm{Gal}(L/L^G)| = [L : L^G] = m \leq n$, da cui $m = n$ e $G = \mathrm{Gal}(L/L^G)$.
Se invece $|G| = +\infty$, banalmente si ha $G < \mathrm{Aut}_{L^G}(L) = \mathrm{Gal}(L/L^G)$. □

Corollario 2.1.3. *L/K normale e $G = \mathrm{Aut}_K(L)$. Allora L/L^G è di Galois e $G = \mathrm{Gal}(L/L^G)$. Inoltre $L^G = K_i$ e, se L/K è separabile, $K = L^G$.*

Dimostrazione. Per una proposizione vista, $L^G = K_i$ e dunque L/L^G è di Galois.
Inoltre per la proposizione precedente $\mathrm{Aut}_K(L) = G < \mathrm{Gal}(L/L^G) = \mathrm{Aut}_{L^G}(L) < \mathrm{Aut}_K(L)$.
□

Teorema 2.1.4 (Corrispondenza di Galois - I parte)**.** *L/K di Galois, $G = \mathrm{Gal}(L/K)$. Esistono due mappe:*

$$\{H \mid H < G\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{F \mid K \subseteq F \subseteq L\}$$

con $\phi(H) = L^H$ e $\psi(F) = \mathrm{Gal}(L/F)$ tali che $\phi \circ \psi = \mathrm{id}$, cioè tali che ψ è iniettiva e ϕ surgettiva.
Se inoltre $|G| < +\infty$, allora anche $\psi \circ \phi = \mathrm{id}$, cioè ϕ e ψ sono bigettive.
Infine, vale in generale che F/K è di Galois $\iff \mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K)$ e in tal caso:

$$\mathrm{Gal}(F/K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)};$$

se inoltre $|G| < +\infty$, allora $H \triangleleft G \iff L^H/K$ è di Galois.

Dimostrazione. Innanzitutto ϕ e ψ sono ben definite e si ha:

$$\phi(\psi(F)) = \phi(\mathrm{Gal}(L/F)) = L^{\mathrm{Gal}(L/F)} = F$$

per il corollario. Se inoltre $|G| < +\infty$, per la proposizione si ha:

$$\psi(\phi(H)) = \psi(L^H) = \mathrm{Gal}(L/L^H) = H.$$

Per la seconda parte, sappiamo che F/K è di Galois $\iff \sigma(F) = F\ \forall \sigma : F \to \overline{K}, \sigma_{|K} = \mathrm{id} \iff \sigma(F) = F\ \forall \sigma \in \mathrm{Gal}(L/K)$; d'altronde $\mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K) \iff \sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/F)\ \forall \sigma \in \mathrm{Gal}(L/K)$.
Notato che $\sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/\sigma(F))$ e che $\sigma(F) = F\ \forall \sigma \in \mathrm{Gal}(L/F) \iff \mathrm{Gal}(L/\sigma(F)) = \mathrm{Gal}(L/F)\ \forall \sigma \in \mathrm{Gal}(L/F)$ per iniettività di ψ, otteniamo quanto voluto.
Inoltre, presa la mappa di restrizione:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(F/K) \\ \sigma & \longmapsto & \sigma_{|F} \end{array}$$

che sappiamo essere surgettiva, per il primo teorema di omomorfismo abbiamo:

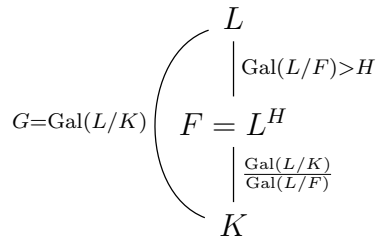
$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} \xrightarrow{\sim} \mathrm{Gal}(F/K)$$

in quanto $\mathrm{Gal}(L/F)$ è esattamente il nucleo della restrizione. □

Vediamo che effettivamente in generale, per estensioni infinite non è vero che ϕ è iniettiva (e dunque ψ surgettiva); vediamo un esempio.

Esempio. Consideriamo $\overline{\mathbb{F}_p}/\mathbb{F}_p$, e sia $G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ gruppo assoluto di Galois di $\mathbb{F}_p$. Sicuramente $\overline{\mathbb{F}_p}^G = \mathbb{F}_p$.
Sia ϕ il Frobenius di $\overline{\mathbb{F}_p}$; allora, posto $H = \langle\phi\rangle < G$, si ha che $\overline{\mathbb{F}_p}^H = \mathbb{F}_p$, dunque se vedo che $H \lneq G$ ho finito (perché avrei mostrato che esistono due sottogruppi di G che fissano lo stesso campo).
$H \cong \mathbb{Z}$, quindi tutti i suoi sottogruppi hanno indice finito; se si avesse che $H = G$ allora ogni sottocampo proprio F di $\overline{\mathbb{F}_p}/\mathbb{F}_p$ avrebbe grado $[F : \mathbb{F}_p]$ finito.
Ma questo è falso, perché se $F = \bigcup_{n\geq 1} \mathbb{F}_{p^{2^n}}$, si ha che $[\overline{\mathbb{F}_p} : F]$ e $[F : \mathbb{F}_p]$ sono infiniti.

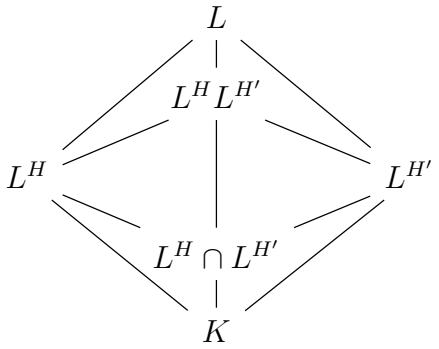
Dunque in generale abbiamo un diagramma:



Corollario 2.1.5. *L/K finita e separabile. Allora L/K ha un numero finito di estensioni intermedie, dunque è semplice.*

Dimostrazione. La chiusura normale $\widetilde{L}/K$ è di Galois finita, quindi le estensioni intermedie sono tante quante i sottogruppi di $\mathrm{Gal}(\widetilde{L}/K)$, che sono in numero finito. □

Corollario 2.1.6. *L/K di Galois finita, $G = \mathrm{Gal}(L/K)$. Consideriamo il diagramma:*



Allora:

1. $L^H \subseteq L^{H'} \iff H \supseteq H'$.
2. $L^H L^{H'} = L^{H \cap H'}$.
3. $L^H \cap L^{H'} = L^{\langle H, H' \rangle}$.

Dimostrazione. 1. Ovvio per il teorema di corrispondenza di Galois.

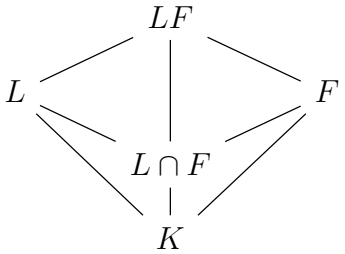
2. $H \cap H' \subseteq H, H'$, dunque $L^{H \cap H'} \supseteq L^H, L^{H'}$ e perciò $L^{H \cap H'} \supseteq L^H L^{H'}$.
   D'altra parte $\mathrm{Gal}(L/L^H L^{H'}) \subseteq \mathrm{Gal}(L/L^H) \cap \mathrm{Gal}(L/L^{H'})$, quindi passando ai campi fissati otteniamo $L^H L^{H'} \supseteq L^{H \cap H'}$.

3. Analoga.

□

Il seguente teorema vale in generale anche per estensioni infinite, ma ancora non siamo in grado di dimostrarlo; vediamolo dunque solo per estensioni di Galois finite:

Teorema 2.1.7. *L/K di Galois finita, $F \supseteq K$, $L, F \subseteq \Omega$. Allora LF/F è di Galois.*



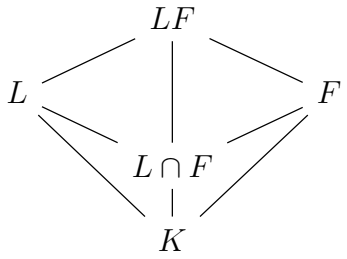
Inoltre $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F)$ *e dunque* $[LF : F] = [L : L \cap F] \mid [L : K]$.

Dimostrazione. LF/F è di Galois perché normalità e separabilità si conservano nel traslato.
La mappa:

$$\begin{array}{rccc} \psi : & \mathrm{Gal}(LF/F) & \longrightarrow & \mathrm{Gal}(L/L \cap F) \\ & \sigma & \longmapsto & \sigma_{|L} \end{array}$$

è ben definita, in quanto se $\sigma_{|L} : L \to \overline{F}$, in realtà $\sigma_{|L} : L \to \overline{K}$, in quanto L/K è algebrica e σ manda elementi algebrici in elementi algebrici, e dunque $\sigma_{|L} : L \to L$ per normalità di L.
Inoltre ψ è iniettiva, perché se σ, σ' coincidessero su L, coinciderebbero anche su LF (in quanto sono l'identità su F).
Per vedere la surgettività di ψ, sia $H = \psi(\mathrm{Gal}(LF/F))$; se vediamo che H e $\mathrm{Gal}(L/L \cap F)$ fissano lo stesso campo avremmo la tesi per la corrispondenza di Galois.
$H < \mathrm{Gal}(L/L \cap F)$, quindi $L^H \supseteq L \cap F$; viceversa sia $\alpha \in L^H \subseteq L$. Per definizione di H, $\forall \sigma \in \mathrm{Gal}(LF/F)$, $\sigma_{|L}(\alpha) = \alpha$, quindi α sta nel sottocampo di LF fissato da $\mathrm{Gal}(LF/F)$, che è F, da cui la tesi. □

Teorema 2.1.8. *L/K e F/K di Galois. Allora LF/K è di Galois.*



Inoltre la mappa:

$$\begin{array}{rccc} \psi: & \mathrm{Gal}(LF/K) & \longrightarrow & \mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K) \\ & \sigma & \longmapsto & (\sigma_{|L},\sigma_{|F}) \end{array}$$

è iniettiva e, se $K = L\cap F$, è bigettiva; se L/K e F/K sono finite, vale anche il viceversa, cioè ψ è bigettiva $\iff K = L\cap F$.

Dimostrazione. LF/K è di Galois perché normalità e separabilità si conservano nel composto. Sicuramente ψ è iniettiva, perché se σ e σ' coincidono su L e F, coincidono anche sul composto LF. Ma presa $\sigma_1 \in \mathrm{Gal}(L/K)$ e $\sigma_2 \in \mathrm{Gal}(F/K)$ tali che $\sigma_{1|L\cap F} = \sigma_{2|L\cap F}$, si può costruire un ben definito $\sigma : LF \to LF$ che estende σ_1 e σ_2 a un omomorfismo di anelli, che sarà un elemento del gruppo di Galois $\mathrm{Gal}(LF/K)$; dunque:

$$\psi(\mathrm{Gal}(LF/K)) = \{(\sigma_1,\sigma_2)\in\mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K) \mid \sigma_{1|L\cap F} = \sigma_{2|L\cap F}\}.$$

Se $L\cap F = K$, per quanto appena detto ψ è surgettivo.
Se inoltre le estensioni sono finite, ψ è bigettiva $\iff |\mathrm{Gal}(LF/K)| = |\mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K)| \iff [LF:K] = [L:K]\cdot[F:K] \iff [F:L\cap F] = [F:K] \iff K = L\cap F$ per la proposizione precedente. □

Proposizione 2.1.9. *$f \in K[x]$, $\deg f = n$, L campo di spezzamento di f su K, $L = K(\alpha_1,\dots,\alpha_n)$. Allora la mappa:*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \hookrightarrow & \mathcal{S}(\{\alpha_1,\dots,\alpha_n\}) \cong \mathcal{S}_n \\ \sigma & \longmapsto & \sigma_{|\{\alpha_1,\dots,\alpha_n\}} \end{array}$$

è un'immersione, dunque $\mathrm{Gal}(L/K) < \mathcal{S}_n$ e $[L:K] \mid n!$.
Inoltre f è irriducibile $\iff \mathrm{Gal}(L/K)$ agisce transitivamente su $\{\alpha_1,\dots\alpha_n\}$.

Dimostrazione. La prima parte è del tutto ovvia, in quanto se un elemento del gruppo di Galois fissa i generatori allora fissa tutto L.
Per la seconda, basta osservare che f è irriducibile $\iff$ è polinomio minimo di ogni sua radice e che $\mathrm{Gal}(L/K)$ agisce transitivamente sulle radici del polinomio minimo di un elemento. □

Corollario 2.1.10. *L/K di Galois, $[L:K] = n$. Allora $\mathrm{Gal}(L/K) < \mathcal{S}_n$.*

Dimostrazione. Discende immediatamente dal teorema di Cayley, oppure si ricava osservando che $L = K(\alpha)$ per un certo α per il teorema dell'elemento primitivo e applicando la proposizione precedente a μ_α. □

2.2 Estensioni abeliane e estensioni cicliche. Le estensioni ciclotomiche

Definizione 2.2.1. Un'estensione di Galois si dice **abeliana** se il suo gruppo di Galois è abeliano, **ciclica** se il suo gruppo di Galois è ciclico.

Vediamo come si comportano questi due tipi di estensioni nelle classiche tre situazioni:

Proprietà. 1. Sia le estensioni abeliane che quelle cicliche non si conservano nelle torri; il controesempio dato nel caso delle estensioni normali, cioè:

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

vale anche in questi due casi. Però vale che, dato il diagramma:

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

L/K abeliana (ciclica) $\Rightarrow$ L/F e F/K abeliane (cicliche), in quanto in entrambi i casi ogni sottogruppo del gruppo di Galois è normale e sottogruppi di un gruppo abeliano (ciclico) sono abeliani (ciclici).

2. Sia le estensioni abeliane che quelle cicliche si conservano nel traslato; dato un diagramma:

$$\begin{array}{ccc} & LF & \\ L & & F \\ & K & \end{array}$$

se L/K è abeliana (ciclica), anche LF/F lo è, in quanto $\mathrm{Gal}(LF/F)$ si immerge in $\mathrm{Gal}(L/K)$.

3. Le estensioni abeliane si conservano nel composto, in quanto il gruppo di Galois di LF è un sottogruppo di $\mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$ abeliano, mentre quelle cicliche non si conservano mai (a meno che una fra L/K e F/K non sia banale).

Esercizio. *L algebricamente chiuso, $\sigma \in \mathrm{Aut}(L)$, $K = L^{\langle\sigma\rangle}$. Allora ogni estensione finita di K è ciclica.*

Dimostrazione. Sia F/K finita e perciò algebrica; K (e dunque F) ha una chiusura algebrica $L_0 \subseteq L$ in L, quindi $F \subseteq L_0$ e F/K è separabile, in quanto, preso $\alpha \in F$, $\mu_\alpha \mid \prod_{\sigma \in \mathrm{Aut}_K(L_0)} (x - \sigma(\alpha))$, che è separabile. Supponiamo come primo caso che F/K sia normale; allora F/K è di Galois e $\sigma_{|F} \in \mathrm{Gal}(F/K)$, dunque $\langle\sigma_{|F}\rangle < \mathrm{Gal}(F/K)$.
Ma $\langle\sigma_{|F}\rangle$ è finito e $K = F^{\langle\sigma_{|F}\rangle}$, dunque $\langle\sigma_{|F}\rangle = \mathrm{Gal}(F/K)$.
In generale, sia F/K finita (e dunque separabile); allora $\widetilde{F}/K$ è di Galois finita, quindi per quanto visto è ciclica, perciò anche F/K è ciclica. □

Osservazione. Consideriamo il polinomio $f(x) = x^n - 1$ sul campo K; $U_n = \{\alpha \in \overline{K} \mid \alpha^n = 1\}$ è un gruppo ciclico in quanto sottogruppo moltiplicativo finito di un campo.
Se $\text{char}(K) = 0$ o $\text{char}(K) \nmid n$, allora $|U_n| = n$.
Se $\text{char}(K) = p \mid n$ e $n = p^a m$, $(m, p) = 1$, allora $f(x) = x^{p^a m} - 1 = (x^m - 1)^{p^a}$, dunque $|U_n| = m$.
Inoltre, se $K = \mathbb{F}_q$, allora $K(U_n) = \mathbb{F}_{q^d}$, dove $d = \min\{h \mid U_n \subseteq \mathbb{F}_{q^h}^*\}$, cioè $d = \text{ord}_{(\mathbb{Z}/n\mathbb{Z})^*}(q)$.
In caratteristica 0, $U_n = \langle \zeta_n \rangle$, dove $\zeta_n = e^{\frac{2\pi i}{n}}$.

Proposizione 2.2.1. *$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ e $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Dimostrazione. Sicuramente l'estensione è di Galois, perché è campo di spezzamento di $f(x) = x^n - 1$.
Se $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, allora $\sigma(\zeta_n) = \zeta_n^i$, con $(i, n) = 1$, in quanto si deve avere che $\sigma(\langle \zeta_n \rangle) = \langle \zeta_n \rangle$; quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$.
Per concludere l'uguaglianza devo mostrare che $\mu(\zeta_n^i) = 0 \ \forall (i, n) = 1$, dove $\mu = \mu_{\zeta_n}$ è il polinomio minimo di ζ_n su $\mathbb{Q}$; osservo però che mi basta mostrare che, presa ξ radice di μ e $p \nmid n$, allora ξ^p è radice di μ, in quanto in questo caso avrei, posto $i = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, una successione di radici di μ:

$$\zeta_n \to \zeta_n^{p_1} \to \zeta_n^{p_1^2} \to \cdots \to \zeta_n^{p_1^{e_1}} \to \cdots \to \zeta_n^i$$

per quanto appena visto.
Sia dunque ξ radice di μ e $f(x) = \mu(x)g(x)$; $0 = f(\xi^p) = \mu(\xi^p)g(\xi^p)$, quindi basta vedere che $g(\xi^p) \neq 0$.
Sia per assurdo $g(\xi^p) = 0$; allora $g(x^p)$ ha ξ come radice, e dunque $\mu(x) = \mu_\xi(x) \mid g(x^p)$.
Passando modulo p, si ha $\overline{\mu(x)} \mid \overline{g(x)^p} = \overline{g(x)}^p$, dunque $(\overline{\mu}, \overline{g}) \neq 1$; ma allora $\overline{x^n - 1} = \overline{\mu(x)g(x)}$ ha una radice multipla, assurdo perché la sua derivata è $\overline{nx^{n-1}} \neq 0$ in quanto $p \nmid n$.
Abbiamo dunque $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$; per vedere che il gruppo di Galois è proprio quello, consideriamo la mappa:

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ [i] & \longmapsto & \sigma_i := \{\zeta_n \to \zeta_n^i\} \end{array}$$

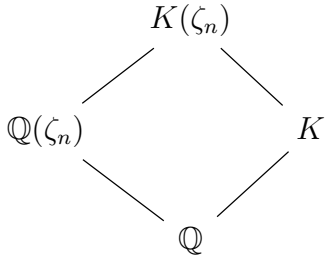
è ben definita e iniettiva per quanto visto, dunque è un isomorfismo per cardinalità. □

Osservazione. Abbiamo le relazioni:

- $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{[n,m]})$;
- $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{(n,m)})$.

Entrambe si dimostrano facilmente con considerazioni sul grado delle estensioni (per la prima si può usare l'identità di Bezout).

Osservazione. Sia $K \supseteq \mathbb{Q}$. Cosa possiamo dire del grado $[K(\zeta_n) : K]$? Consideriamo il diagramma:



Sicuramente $[K(\zeta_n) : K] = d \mid \phi(n)$, perché $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è di Galois.
Inoltre $\mu_{\zeta_n}(x)$ si fattorizza in K come prodotto di $\frac{\phi(n)}{d}$ fattori di grado d, in quanto $K(\zeta_n^i) = K(\zeta_n) \ \forall (i, n) = 1$ e dunque i polinomi minimi di tutti gli ζ_n^i hanno lo stesso grado d.

2.3 Teoria di Galois infinita

Sia L/K una generica estensione di Galois. Definiamo:

$$\mathscr{L}_{L/K} = \{L_i \mid K \subseteq L_i \subseteq L \text{ e } L_i/K \text{ è di Galois finita}\} = \{L_i \mid i \in I\}.$$

Ho che $L = \bigcup_{i\in I} L_i$, poiché se $\alpha \in L$, il campo di spezzamento di μ_α sarà un certo L_i, quindi $\alpha \in L_i$.
Consideriamo le mappe di restrizione:

$$\begin{array}{rccc} \psi_i: & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L_i/K) \\ & \sigma & \longmapsto & \sigma_{|L_i} = \sigma_i \end{array}$$

sappiamo che $\mathrm{Ker}(\psi_i) = \mathrm{Gal}(L/L_i) \triangleleft \mathrm{Gal}(L/K)$; inoltre la mappa:

$$\begin{array}{rccc} \rho: & \mathrm{Gal}(L/K) & \longrightarrow & \prod_{i\in I} \mathrm{Gal}(L_i/K) \\ & \sigma & \longmapsto & \{\sigma_i\}_{i\in I} \end{array}$$

è un omomorfismo iniettivo.
Dico che $\rho(\mathrm{Gal}(L/K)) = \left\{\{\sigma_i\}_{i\in I} \mid \sigma_{j_{|L_i}} = \sigma_i \text{ se } L_i \subseteq L_j\right\}$ (e una tale successione di σ_i si dice coerente): l'inclusione $\subseteq$ è ovvia, in quanto ogni σ_i è restrizione della stessa σ; viceversa, definendo $\sigma(\alpha) = \sigma_i(\alpha)$ con $\alpha \in L_i$ (è una buona definizione per coerenza delle σ_i), si ottiene un elemento del gruppo di Galois $\mathrm{Gal}(L/K)$.

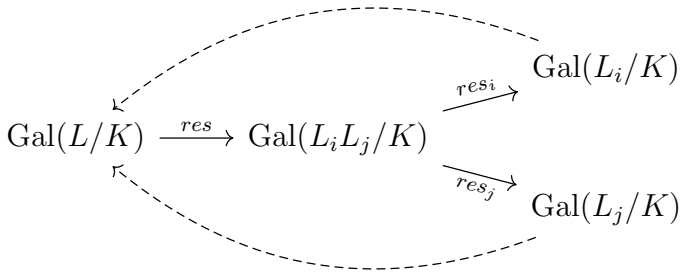
Adesso vogliamo mettere su $\mathrm{Gal}(L/K)$ una topologia; per farlo procediamo per passi. Mettiamo su ogni $\mathrm{Gal}(L_i/K)$ la topologia discreta, su $\prod_{i\in I} \mathrm{Gal}(L_i/K)$ la topologia prodotto, su $\rho(\mathrm{Gal}(L/K)) \subseteq \prod_{i\in I} \mathrm{Gal}(L_i/K)$ la topologia di sottospazio e infine su $\mathrm{Gal}(L/K)$ la topologia indotta da ρ.
Osserviamo che una prebase della topologia prodotto è $\left\{\prod_{i\in I} V_i^{i_0}\right\}_{i_0\in I}$, dove $V_i^{i_0} = \mathrm{Gal}(L_i/K)$ se $i \neq i_0$ e $V_{i_0}^{i_0} = \{\sigma_{i_0}\}$; per definizione di topologia prodotto, le ψ_i (che sono la composizione di una proiezione con ρ) sono continue. Tale topologia su $\mathrm{Gal}(L/K)$ è detta **topologia di Krull**.
Una prebase per la topologia di Krull è data dagli aperti:

$$\rho^{-1}\left(\prod_{i\in I} V_i^{i_0}\right) = \psi_{i_0}^{-1}(\sigma_{i_0}) = \widetilde{\sigma_{i_0}}\,\mathrm{Gal}(L/L_{i_0})$$

classi laterali del nucleo di ψ_{i_0}, dove $\widetilde{\sigma_{i_0}}$ è un'estensione di σ_{i_0} a L. Notiamo però che essa è proprio una base della topologia: per vederlo, prendiamo due tali aperti $\sigma\,\mathrm{Gal}(L/L_i)$ e $\tau\,\mathrm{Gal}(L/L_j)$. La loro intersezione può essere scritta:

$$\begin{aligned} \sigma\,\mathrm{Gal}(L/L_i) \cap \tau\,\mathrm{Gal}(L/L_j) &= \left(\bigcup_{k=1}^{n} \sigma^{(k)}\,\mathrm{Gal}(L/L_iL_j)\right) \cap \left(\bigcup_{h=1}^{m} \tau^{(h)}\,\mathrm{Gal}(L/L_iL_j)\right) = \\ &= \bigcup_{k\in A} \sigma^{(k)}\,\mathrm{Gal}(L/L_iL_j), \end{aligned}$$

con $A \subseteq \{1,\dots,n\}$; per vederlo osserviamo come prima cosa che le composizioni:



mostrano che la fibra (tratteggiata in figura) di un elemento σ di $\mathrm{Gal}(L_i/K)$ (o di $\mathrm{Gal}(L_j/K)$) in $\mathrm{Gal}(L/K)$ è unione delle fibre secondo res delle fibre di σ secondo res_i; inoltre osserviamo che l'intersezione di due classi laterali $\sigma^{(k)}\,\mathrm{Gal}(L/L_iL_j)$ e $\tau^{(h)}\,\mathrm{Gal}(L/L_iL_j)$ può essere:

$$\sigma^{(k)}\,\mathrm{Gal}(L/L_iL_j)\cap\tau^{(h)}\,\mathrm{Gal}(L/L_iL_j)=\begin{cases}\sigma^{(k)}\,\mathrm{Gal}(L/L_iL_j) & \text{se } {\sigma^{(k)}}_{|L_iL_j}={\tau^{(h)}}_{|L_iL_j}\\ \emptyset & \text{altrimenti}\end{cases}$$

Abbiamo dunque una base di aperti fatti da classi laterali di sottogruppi normali.

<u>*Osservazione*</u>. $\mathrm{Gal}(L/K)$ con la topologia di Krull è un gruppo topologico. Infatti, denotata con m la moltiplicazione e con γ l'inversione, basta verificare che m e γ sono continue su una base di aperti.
Ma:

$$m^{-1}(\sigma\,\mathrm{Gal}(L/L_k))=\bigcup_{\tau\in\mathrm{Gal}(L_k/K)}\tau\,\mathrm{Gal}(L/L_k)\times\tau^{-1}\sigma\,\mathrm{Gal}(L/L_k)$$

e:

$$\gamma^{-1}(\sigma\,\mathrm{Gal}(L/L_k))=\sigma^{-1}\,\mathrm{Gal}(L/L_k),$$

dunque entrambe sono funzioni continue.

<u>*Osservazione*</u>. In $\mathrm{Gal}(L/K)$, una base di intorni di 1 è data dai $\{\mathrm{Gal}(L/L_i)\}_{i\in I}$, dunque, sapendo che la moltiplicazione è continua, deduciamo di nuovo che una base di intorni per $\sigma\in\mathrm{Gal}(L/K)$ è $\{\sigma\,\mathrm{Gal}(L/L_i)\}_{i\in I}$.

<u>*Osservazione*</u>. In $\mathrm{Gal}(L/K)$, gli aperti $\mathrm{Gal}(L/L_i)$ sono anche chiusi; infatti in generale, in un gruppo topologico qualsiasi, i sottogruppi aperti sono anche chiusi. Questo può essere visto osservando che, preso $H<G$ aperto:

$$G\backslash H=\bigcup_{\sigma\neq 1}\sigma H$$

è anch'esso aperto, cioè H è chiuso.
Analogamente si mostra che ogni sottogruppo chiuso di indice finito è aperto.

Proposizione 2.3.1. $\mathrm{Gal}(L/K)$ *con la topologia di Krull è di Hausdorff, compatto e totalmente sconnesso.*

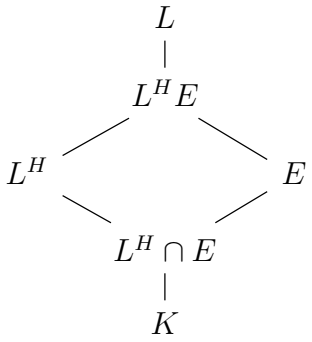
Dimostrazione. Vediamo che è T2; siano $\sigma\neq\tau\in\mathrm{Gal}(L/K)$. σ e τ non coincidono su un certo L_i, poiché altrimenti coinciderebbero su L, dunque $\sigma\,\mathrm{Gal}(L/L_i)\cap\tau\,\mathrm{Gal}(L/L_i)=\emptyset$.
$\mathrm{Gal}(L_i/K)$ è compatto con la topologia discreta perché è finito, dunque $\prod_{i\in I}\mathrm{Gal}(L_i/K)$ è compatto perché prodotto di compatti; se vedo che $\rho(\mathrm{Gal}(L/K))$ è chiuso, sarebbe un chiuso in un compatto e dunque un compatto (e quindi anche $\mathrm{Gal}(L/K)$ sarebbe compatto perché ha la topologia indotta di ρ).
Equivalentemente, mostro che $\prod_{i\in I}\mathrm{Gal}(L/L_i)\backslash\rho(\mathrm{Gal}(L/K))$ è aperto: se $\{\sigma_j\}$ non è coerente, voglio vedere che esiste un suo intorno fatto solo da successioni non coerenti.
Sicuramente $\exists n,m$ tali che $L_n\subseteq L_m$ e $\sigma_{m|L_n}\neq\sigma_n$; prendendo $\prod_{h\in I}V_h$, dove $V_h=\mathrm{Gal}(L_h/K)$ se $h\neq n,m$, $V_n=\{\sigma_n\}$, $V_m=\{\sigma_m\}$, ho un intorno aperto fatto solamente da successioni non coerenti.
Infine $\mathrm{Gal}(L/K)$ è totalmente sconnesso, perché su ogni $\mathrm{Gal}(L_i/K)$ ho messo la topologia discreta e le componenti connesse sono i prodotti delle componenti connesse. □

Lemma 2.3.2. $H<G=\mathrm{Gal}(L/K)$. *Allora* $\mathrm{Gal}(L/L^H)=\overline{H}$ *(dove* $\overline{H}$ *rappresenta la chiusura topologica di* H*).*

Dimostrazione. Mostriamo innanzitutto che $\forall F$ tale che $K \subseteq F \subseteq L$, $\mathrm{Gal}(L/F)$ è chiuso. Consideriamo $X = \{F_i \mid K \subseteq F_i \subseteq F \text{ e } F_i/K \text{ è di Galois finita}\}$; allora:

$$\mathrm{Gal}(L/F) = \bigcap_{F_i \in X} \mathrm{Gal}(L/F_i).$$

Infatti l'inclusione $\subseteq$ è ovvia, in quanto un automorfismo che fissa F_i fissa anche F, mentre se esistesse $\sigma \in \bigcap_{F \in X} \mathrm{Gal}(L/F_i)$ che non fissa F, allora non fisserebbe un $\alpha \in F$; ma sicuramente $\exists i$ tale che $\alpha \in F_i$, e dunque σ fissa α. Perciò $\mathrm{Gal}(L/F)$ è chiuso in quanto intersezione di chiusi.
$H \subseteq \mathrm{Gal}(L/L^H)$, che è chiuso, quindi $\overline{H} \subseteq \mathrm{Gal}(L/L^H)$.
Viceversa, sia $\sigma \in \mathrm{Gal}(L/L^H)$. Presa E/K finita e di Galois, devo vedere che $\exists h \in H$ tale che σ e h coincidono su E, cioè $h\,\mathrm{Gal}(L/E) = \sigma\,\mathrm{Gal}(L/E)$. Ma dato il diagramma:

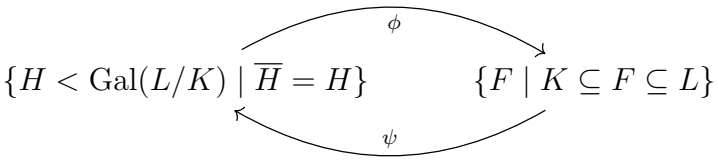


visto che E/K (e dunque $E/L^H \cap E$) è finita, si ha $\mathrm{Gal}(L^H E/L^H) \cong \mathrm{Gal}(E/L^H \cap E)$ e perciò basta vedere che $\exists h \in H$ tale che σ e h coincidono su $L^H E$.
Sia quindi F tale che $L^H \subseteq F \subseteq L$ e F/L^H è finita e di Galois (F sta ad indicare l'$L^H E$ precedente); consideriamo:

$$\begin{array}{rccc} res: & H & \longrightarrow & \mathrm{Gal}(F/L^H) \\ & \tau & \longmapsto & \tau_{|F} \end{array}$$

$F^{res(H)} = L^H$, quindi per la teoria di Galois finita $res(H) = \mathrm{Gal}(F/L^H)$; dunque $\exists \tau \in H$ tale che $\tau_{|F} = \sigma_{|F}$, cioè $\tau \in H \cap \sigma\,\mathrm{Gal}(L/F)$.
Ma allora l'intersezione di ogni intorno di σ con H è diversa dal vuoto, cioè la tesi. □

Teorema 2.3.3 (Corrispondenza di Galois - II parte)**.** *L/K di Galois. Le mappe:*



sono l'una l'inversa dell'altra, e in particolare sono bigettive.

Dimostrazione. Visto che $\mathrm{Gal}(L/F)$ è chiuso $\forall F$ come visto nel lemma, segue che $\phi \circ \psi = \mathrm{id}$, in quanto questo era già stato mostrato nella I parte.
Ma per il lemma ψ è surgettiva, quindi segue la tesi. □

Proposizione 2.3.4. *Un sottogruppo H di $\mathrm{Gal}(L/K)$ è aperto $\iff$ è chiuso e $[L^H : K] < +\infty$*

Dimostrazione. Sicuramente i sottogruppi H aperti hanno indice finito, perché $G = \bigsqcup \sigma H$ e G è compatto, quindi $\#\{\sigma H\} < +\infty$. Ma se $F = L^H$, $[F : K] = \left|\frac{G}{H}\right|$, perché $[F : K] = |\mathrm{Hom}_K(F, \overline{K})|$ e c'è la corrispondenza biunivoca:

$$\begin{array}{ccc} \mathrm{Hom}_K(F, \overline{K}) & \longrightarrow & \frac{G}{H} \\ \sigma_i & \longmapsto & \widetilde{\sigma}_i H \end{array}$$

dove $\widetilde{\sigma_i}$ è una qualunque estensione di σ_i a G.
D'altra parte le implicazioni H aperto $\Rightarrow$ H chiuso e H chiuso di indice finito $\Rightarrow$ H aperto sono già state viste, quindi segue la tesi. □

Osservazione. In generale l'implicazione $H < \mathrm{Gal}(L/K)$ sottogruppo di indice finito $\Rightarrow$ H aperto è falsa.

Vogliamo adesso classificare i gruppi di Galois infiniti all'interno dei gruppi profiniti, e dar loro una caratterizzazione come limiti proiettivi:

Definizione 2.3.1. G gruppo topologico si dice **profinito** se è T2, compatto e ha una base di intorni di 1 fatta da sottogruppi normali.

Osservazione. I gruppi di Galois sono gruppi profiniti; inoltre tutti i gruppi finiti con la topologia discreta sono profiniti.

Osservazione. Tutti i gruppi profiniti (e dunque tutti i gruppi di Galois) infiniti non sono numerabili. Infatti se G è profinito e numerabile, vogliamo vedere che tutti i punti sono isolati (quindi G è discreto e compatto e dunque finito).
Sia $G = \{x_1, x_2, \ldots\}$; visto che i punti sono chiusi, per mostrare che sono isolati basta vedere che sono anche aperti. Ma se per assurdo $G\backslash\{x_i\}$ non fosse chiuso, sarebbe un aperto denso $\forall i$, quindi per il teorema di Baire l'intersezione numerabile $\bigcap_{i=1}^{\infty} G\backslash\{x_i\} = \emptyset$ sarebbe densa, assurdo.

Definizione 2.3.2. I insieme di indici con l'ordine parziale $\leq$. $(I, \leq)$ si dice **diretto** se $\forall i, j \in I$ $\exists k \in I$ tale che $i, j \leq k$.

Definizione 2.3.3. Un **sistema proiettivo** su I diretto è una famiglia $\{G_i, f_{ij}\}_{i \leq j}$, con $G_i \in \mathrm{Obj}(\mathcal{C})$ oggetti di una certa categoria $\mathcal{C}$ e, $\forall i \leq j$, $f_{ij} : G_j \to G_i \in \mathrm{Hom}(\mathcal{C})$ è un morfismo di $\mathcal{C}$ tale che $f_{ii} = \mathrm{id}$ $\forall i \in I$ e il diagramma:

$$\begin{array}{ccc} G_j & \xrightarrow{f_{ij}} & G_i \\ {\scriptstyle f_{jk}}\uparrow & \nearrow_{f_{ik}} & \\ G_k & & \end{array}$$

commuta $\forall i \leq j \leq k$.

Definizione 2.3.4. Il **limite proiettivo** del sistema proiettivo $\{G_i, f_{ij}\}_{i \leq j}$ è l'elemento universale della categoria $\mathcal{C}$ per il sistema, cioè è l'elemento $\{G = \varprojlim G_i, f_i\}$, con $f_i : G \to G_i$ tale che il diagramma

$$\begin{array}{ccc} G & \xrightarrow{f_i} & G_i \\ {\scriptstyle f_j}\downarrow & \nearrow_{f_{ij}} & \\ G_j & & \end{array}$$

commuta $\forall i \leq j$, tale che, $\forall\{L, \psi_i\}$ con la precedente proprietà, $\exists!\varphi : L \to G$ tale che:

$$\begin{array}{ccccc} L & & \xrightarrow{\varphi} & & G \\ & {\scriptstyle \psi_i}\searrow & & \swarrow{\scriptstyle f_i} & \\ & & G_i & & \end{array}$$

commuta $\forall i$.

Si può mostrare che l'elemento universale rispetto a una certa famiglia di oggetti è unico

Osservazione. Nel nostro caso, la categoria $\mathcal{C}$ è la categoria dei gruppi topologici, con morfismi gli omomorfismi continui; inoltre:

$$\varprojlim G_i = \left\{ \{\sigma_i\}_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; f_{ij}(\sigma_j) = \sigma_i \ \forall i \leq j \right\},$$

in quanto questo soddisfa le ipotesi e l'elemento universale è unico.

Osservazione. Abbiamo visto che $\mathrm{Gal}(L/K) = \{\{\sigma_i\} \in \mathrm{Gal}(L_i/K)$ coerenti, con L_i/K finita e di Galois$\}$; dunque:

$$\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(L_i/K)$$

dove $i \leq j$ se $L_i \subseteq L_j$ e $f_{ij} : \mathrm{Gal}(L_j/K) \to \mathrm{Gal}(L_i/K)$ è la restrizione.

Osservazione. Se i G_i sono T2, allora il loro limite proiettivo G è T2 e chiuso nel prodotto dei G_i; la dimostrazione è analoga a quella vista per i gruppi di Galois.

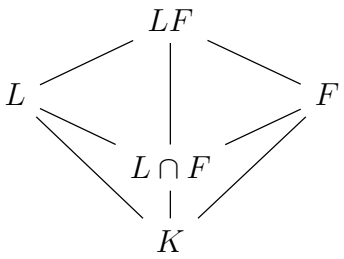
In realtà vale il seguente teorema, che non dimostriamo:

Teorema 2.3.5. *Ogni gruppo profinito è il limite proiettivo di una certa famiglia di gruppi finiti con la topologia discreta. In particolare:*

- *Se G è profinito e $\{N_i\} = \{$sottogruppi normali aperti di $G\}$, allora $G \cong \varprojlim \frac{G}{N_i}$, dove $\cong$ indica che sono sia isomorfi sia omeomorfi;*
- *Se $\{G_i, f_{ij}\}$ è un sistema proiettivo di gruppi finiti con la topologia discreta, allora il gruppo $G = \varprojlim G_i$ è profinito.*

Siamo adesso pronti per estendere un teorema giá visto nel caso finito anche al caso infinito:

Teorema 2.3.6. *L/K di Galois, $F \supseteq K$, $L, F \subseteq \Omega$. Allora LF/F è di Galois.*



Inoltre $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F)$.

Dimostrazione. Scrivendo $L = \prod_i L_i$, dove $L_i/L \cap F$ é finita e di Galois, si ha che per ogni i, $\mathrm{Gal}(L_i/L \cap F) \cong \mathrm{Gal}(L_iF/F)$ per il caso finito. Scrivendo $\mathrm{Gal}(L/L \cap F) = \varprojlim \mathrm{Gal}(L_i/L \cap F)$, gli isomorfismi $\psi_i : \mathrm{Gal}(L_iF/F) \xrightarrow{\sim} \mathrm{Gal}(L_i/L \cap F)$ passano al limite proiettivo definendo la controimmagine di $\sigma \in \mathrm{Gal}(L/L \cap F)$ come la successione coerente delle controimmagini $\psi_i^{-1}(\sigma_{|L_i})$. □

Concludiamo la sezione con i calcoli espliciti di qualche gruppo di Galois infinito:

Esempi. 1. $\{\mathbb{Z}/p^n\mathbb{Z}, \pi_{nm}\}$, dove $\pi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, con $n \leq m$, è la proiezione, è un sistema proiettivo. Denotiamo:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ \{a_i\} \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\},$$

cioè un elemento di $\mathbb{Z}_p$ è del tipo:

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \dots \\ (a_0, & & a_0 + pa_1, & & a_0 + pa_1 + p^2a_2, & & \dots \end{array}$$

che identifichiamo come la serie $\sum_{i\geq 0} a_i p^i$. Gli elementi dell'anello $\mathbb{Z}_p$ sono detti **interi p-adici**.

2. $\{\mathbb{Z}/n\mathbb{Z}, \pi_{nm}\}$, dove $n \leq m$ se $n \mid m$ e $\pi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ è la proiezione, è un sistema proiettivo. Denotiamo:
$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \varprojlim \mathbb{Z}/(n!)\mathbb{Z}.$$

Proposizione 2.3.7. $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

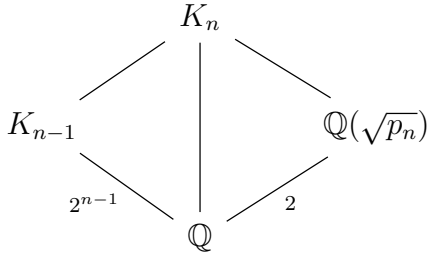
Dimostrazione. La mappa:
$$\begin{array}{rccc} \varphi : & \hat{\mathbb{Z}} & \longrightarrow & \prod_p \mathbb{Z}_p \\ & \{\sigma_i\} & \longmapsto & \{\{\sigma_{p^n}\}_n\}_p \end{array}$$
è ben definita, poiché successioni coerenti vanno in successioni coerenti.
Vediamo che φ è iniettiva; sia $\{\sigma_n\}$ tale che $\varphi(\{\sigma_n\}) = \{\{0\}\}$, cioè tale che $\sigma_{p^n} = 0\ \forall p, n$.
Sia $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$; vogliamo vedere che $\sigma_m = 0$. Visto che sappiamo che $\sigma_{p_i^{e_i}} = 0\ \forall i$, e che $\sigma_m \equiv \sigma_{p_i^{e_i}} \equiv 0\ (p_i^{e_i})\ \forall i = 1, \ldots, r$, allora per il teorema cinese $\sigma_m \equiv 0\ (m)$.
Vediamo invece che φ è surgettiva; sia $\{\{\sigma_{p^a}\}_a\}_p$.
Cerco $\{\sigma_n\}$ tale che, se $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, $\sigma_n \equiv \sigma_{p_i^{e_i}}\ (p_i^{e_i})\ \forall i$. Tale sistema ha soluzione per il teorema cinese, e si può verificare che tale soluzione è coerente.
Infine φ è un omeomorfismo perché intorni di $\{\sigma_n\}$ vanno in intorni di $\varphi(\{\sigma_n\})$. □

Esempio. $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z}$, con omomorfismi le restrizioni $res_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$; i diagrammi:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) & \xrightarrow{res_{nm}} & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \updownarrow \psi_m & & \updownarrow \psi_n \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\pi_{nm}]{} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

commutano, quindi $\varprojlim \{\mathbb{Z}/n\mathbb{Z}, res_{nm}\} \cong \varprojlim \{\mathbb{Z}/n\mathbb{Z}, \pi_{nm}\}$, cioè $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$.
Osservazione. Se $K_n = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, con $p_1, \ldots, p_n$ primi distinti o -1, allora:
$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

Dimostrazione. Procediamo per induzione su n, essendo il caso $n = 1$ evidente.
Se $n > 1$, consideriamo il diagramma:



$K_{n-1} \cap \mathbb{Q}(\sqrt{p_n}) = \mathbb{Q}$, quindi, per quanto visto, basta mostrare che $\mathbb{Q}(\sqrt{p_n}) \not\subseteq K_{n-1}$.
Le sottoestensioni di K_{n-1} di grado 2 sono tante quanti i sottogruppi di $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ di indice 2,

cioè $2^{n-1}-1$ (infatti i sottogruppi di indice 2, che sono gli iperpiani di $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ come spazio vettoriale su $\mathbb{F}_2$, sono tanti quanti i sottogruppi di ordine 2, che sono le rette di $(\mathbb{Z}/2\mathbb{Z})^{n-1}$, per un ragionamento di dualità).
Ma le sottoestensioni del tipo $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1}\cdot\ldots\cdot p_{n-1}^{\varepsilon_{n-1}}})$, con $\varepsilon_i \in \{0,1\}$ sono esattamente 2^{n-1} ($2^{n-1}-1$ se non si conta $\mathbb{Q}$) e sono tutte distinte, in quanto due estensioni quadratiche $\mathbb{Q}(\sqrt{n})$ e $\mathbb{Q}(\sqrt{m})$ di $\mathbb{Q}$ sono la stessa $\iff$ nm è un quadrato.
Segue perciò che $\mathbb{Q}(\sqrt{p_n})$ non è una sottoestensione di K_{n-1}, cioè la tesi. □

Esempio. Sia $L = \mathbb{Q}(\sqrt{m} \mid m \in \mathbb{Q})$. Allora $L = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\} \cup \{\sqrt{-1}\})$ e dunque $\mathrm{Gal}(L/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $L/\mathbb{Q}$.
Ma visto che i K_n sono una sottofamiglia filtrante delle F_i, cioè $\forall i\ \exists n$ tale che $F_i \subseteq K_n$, allora $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$.
Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

$$\mathrm{Gal}(L/K) \cong \varprojlim (\mathbb{Z}/2\mathbb{Z})^n \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z},$$

in quanto si identifica una successione $\{a_n \in (\mathbb{Z}/2\mathbb{Z})^n\}_n$ con il suo elemento limite in $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

Esempio. Vogliamo trovare tutte le sottoestensioni di $\overline{\mathbb{F}_p}/\mathbb{F}_p$ (o equivalentemente tutti i sottogruppi chiusi di $\hat{\mathbb{Z}}$). Se q è un primo, denoto $L_q = \bigcup_{n\geq 0} \mathbb{F}_{p^{q^n}}$; si osserva che $[L_q : \mathbb{F}_p] = [\overline{\mathbb{F}_p} : L_q] = +\infty$ e $\mathrm{Gal}(L_q/\mathbb{F}_p) \cong \mathbb{Z}_q$.
Sia F un campo tale che $\mathbb{F}_p \subseteq F \subseteq L_q$; considero $\sup\{[\mathbb{F}_p(x) : \mathbb{F}_p] \mid x \in F\} = q^{n_F}$, con $0 \leq n_F \leq \infty$. Dico che $F = \mathbb{F}_{p^{q^{n_F}}}$ (con la convenzione che $L_q = \mathbb{F}_{p^{q^\infty}}$):

$\subseteq$) Se $n_F = \infty$ è ovvio, mentre se $n_F < \infty$ vale in quanto $[\mathbb{F}_p(x) : \mathbb{F}_p] \mid q^{n_F}\ \forall x \in F$;

$\supseteq$) Se $n_F < \infty$, allora $\exists x \in F$ tale che $[\mathbb{F}_p(x) : \mathbb{F}_p] = q^{n_F}$, dunque $F \supseteq \mathbb{F}_p(x) = \mathbb{F}_{p^{q^{n_F}}}$; se $n_F = \infty$, allora l'estremo superiore è $> n\ \forall n$, cioè esistono elementi in F di grado arbitrariamente grande su $\mathbb{F}_p$, cioè $F \supseteq \mathbb{F}_{p^{q^n}}\ \forall n \geq 0$.

Ne ricaviamo che i sottogruppi chiusi di $\mathbb{Z}_q$ sono i gruppi di Galois $\mathrm{Gal}(L_q/\mathbb{F}_{p^{q^n}})$ al variare di $n \in \mathbb{N} \cup \{\infty\}$; consideriamo solo $n \in \mathbb{N}$, in quanto se $n = \infty$ il gruppo di Galois viene banale.
Detto ϕ il Frobenius di $L_q/\mathbb{F}_p$, si ha che $\mathbb{Z}_q \cong \mathrm{Gal}(L_q/\mathbb{F}_p) = \overline{\langle\phi\rangle}$; inoltre $\langle\phi^{q^n}\rangle$ fissa $\mathbb{F}_{p^{q^n}}$ ma non $\mathbb{F}_{p^{q^{n+1}}}$, dunque $\overline{\langle\phi^{q^n}\rangle} = \mathrm{Gal}(L_q/\mathbb{F}_{p^{q^n}})$. Ma se φ è l'isomorfismo:

$$\begin{array}{rccc} \varphi: & \overline{\langle\phi\rangle} & \xrightarrow{\sim} & \mathbb{Z}_q \\ & \phi & \longmapsto & 1 \end{array},$$

allora la restrizione di φ a $\overline{\langle\phi^{q^n}\rangle}$ dà un isomorfismo:

$$\begin{array}{rccc} \varphi_{|\overline{\langle\phi^{q^n}\rangle}}: & \overline{\langle\phi^{q^n}\rangle} & \xrightarrow{\sim} & q^n\mathbb{Z}_q \\ & \phi^{q^n} & \longmapsto & q^n \end{array},$$

da cui si deduce che $\mathrm{Gal}(L_q/\mathbb{F}_{p^{q^n}}) \cong q^n\mathbb{Z}_q$; per quanto visto prima otteniamo anche che i sottogruppi chiusi di $\mathbb{Z}_q$ (con la topologia indotta come limite proiettivo) sono della forma $q^n\mathbb{Z}_q$, con $n \in \mathbb{N} \cup \{\infty\}$ (e la convenzione $q^\infty\mathbb{Z}_q = \{0\}$).
Passiamo ora al caso generale di un'estensione intermedia K di $\overline{\mathbb{F}_p}/\mathbb{F}_p$; preso un qualunque primo q, denotiamo $K^{(q)} = K \cap L_q$. Allora si ha:

$$K = \prod_q K^{(q)}.$$

$\supseteq$) Ovvia, in quanto ciascuno dei $K^{(q)}$ è contenuto in K.

$\subseteq$) Sia $x \in K$, e diciamo che $[\mathbb{F}_p(x) : \mathbb{F}_p] = m$, con $m = q_1^{e_1} \cdot \ldots \cdot q_r^{e_r}$; allora $x \in \mathbb{F}_{p^m} = \prod_i \mathbb{F}_{p^{q_i^{e_i}}} \subseteq \prod_i K^{(q_i)}$.

Perciò per quanto visto prima $K^{(q)} = \mathbb{F}_{p^{q^{n_q}}}$ per un certo $n_q \in \mathbb{N} \cup \{\infty\}$, da cui:

$$K = \prod_q \mathbb{F}_{p^{q^{n_q}}}.$$

Ma le estensioni $\mathbb{F}_{p^{q^{n_q}}}$ hanno a due a due intersezione banale (cioè $\mathbb{F}_p$), quindi segue che:

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/K) \cong \prod_q q^{n_q}\mathbb{Z}_q,$$

in quanto $\prod_q q^{n_q}\mathbb{Z}_q = \bigcap_q \left((q^{n_q}\mathbb{Z}_q) \prod_{p \neq q} \mathbb{Z}_p\right)$ è chiuso perché intersezione di chiusi.
Concludiamo che i sottogruppi chiusi di $\hat{\mathbb{Z}}$ sono quelli del tipo:

$$\prod_q q^{n_q}\mathbb{Z}_q = \bigcap_q \left((q^{n_q}\mathbb{Z}_q) \prod_{p \neq q} \mathbb{Z}_p\right),$$

con $n_q \in \mathbb{N} \cup \{\infty\}$ (e con la convezione precedente).
Se definiamo i **numeri supernaturali** (o **di Steinitz**) come prodotti formali del tipo $\prod_q q^{n_q}$ con $n_q \in \mathbb{N} \cup \{\infty\}$, allora i sottogruppi chiusi di $\hat{\mathbb{Z}}$ (e le estensioni intermedie di $\overline{\mathbb{F}_p}/\mathbb{F}_p$) sono in corrispondenza biunivoca con i numeri supernaturali:

$$\begin{array}{ccc} S\mathbb{N} & \longrightarrow & \{\text{sottogruppi chiusi di } \hat{\mathbb{Z}}\} \\ \prod_q q^{n_q} & \longmapsto & \left(\prod_q q^{n_q}\right)\hat{\mathbb{Z}} = \prod_q q^{n_q}\mathbb{Z}_q \end{array}$$

in quanto $\left(\prod_q q^{n_q}\right)\hat{\mathbb{Z}} = \prod_q q^{n_q} \prod_q \mathbb{Z}_q = \prod_q q^{n_q}\mathbb{Z}_q$ (infatti $p\mathbb{Z}_q \cong \mathbb{Z}_q \ \forall p$ coprimo con q perché essendo p invertibile modulo q, la moltiplicazione per p è un automorfismo di $\mathbb{Z}_q$).

2.4 Teoria inversa di Galois

La teoria inversa di Galois studia quali gruppi si realizzano come gruppi di Galois, cioè cerca i gruppi G per cui $\exists L \supseteq K$ tale che $\mathrm{Gal}(L/K) \cong G$, con K fissato.
La parte più interessante della teoria si occupa della realizzabilità su $\mathbb{Q}$; questa ricerca nasce dello studio del gruppo (ancora per lo più sconosciuto) $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in quanto i quozienti di $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sono esattamente i gruppi realizzabili come gruppi di Galois su $\mathbb{Q}$.

L'obiettivo di questa sezione è mostrare che i gruppi abeliani finiti e i gruppi simmetrici sono realizzabili come gruppi di Galois su $\mathbb{Q}$. Iniziamo innanzitutto a vederlo per i gruppi abeliani; per farlo abbiamo bisogno di un importante teorema (caso particolare del teorema di Dirichlet), che non dimostriamo:

Teorema 2.4.1. *Preso $n \in \mathbb{N}$, esistono infiniti primi nella progressione aritmetica $1 + kn$, cioè esistono infiniti primi p congrui a 1 modulo n.*

Proposizione 2.4.2. *I gruppi abeliani finiti si realizzano come gruppi di Galois su $\mathbb{Q}$.*

Dimostrazione. Vediamo innanzitutto che la tesi vale per i gruppi ciclici finiti; sia $n \in \mathbb{N}$ e $p \equiv 1 \quad (n)$ primo. Visto che $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$, esso conterrà un (unico) quoziente G/H isomorfo a $\mathbb{Z}/n\mathbb{Z}$, dunque, indicato $F = \mathbb{Q}(\zeta_p)^H$, si ha che F è il campo voluto. In generale, se $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ vediamo per induzione su k che G è realizzabile su $\mathbb{Q}$ (il passo base è appena stato fatto).
Se F_k è tale che $\mathrm{Gal}(F_k/\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ ed ho preso $\mathbb{Z}/n_i\mathbb{Z}$ come quoziente del gruppo di Galois di $\mathbb{Q}(\zeta_{p_i})$ su $\mathbb{Q}$, con $p_i \equiv 1 \quad (n_i)$, allora scelgo $p_{k+1} \equiv 1 \quad (n_{k+1})$ tale che $p_{k+1} \notin \{p_1, \ldots, p_k\}$; in questo modo, detto F il sottocampo di $\mathbb{Q}(\zeta_{p_{k+1}})$ con gruppo di Galois su $\mathbb{Q}$ isomorfo a $\mathbb{Z}/n_{k+1}\mathbb{Z}$, si ha $\mathrm{Gal}(F_k \times F) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_{k+1}\mathbb{Z}$ (in quanto $F_k \cap F \subseteq \prod_{i=1}^k \mathbb{Q}(\zeta_{p_i}) \cap \mathbb{Q}(\zeta_{p_{k+1}}) = \prod_{i=1}^k \left(\mathbb{Q}(\zeta_{p_i}) \cap \mathbb{Q}(\zeta_{p_{k+1}})\right) = \prod_{i=1}^k \mathbb{Q}(\zeta_{(p_i, p_{k+1})}) = \mathbb{Q}$). □

Osservazione. $\mathbb{Z}$ non si realizza come gruppo di Galois perché non è profinito, in quanto non coincide con la sua **chiusura proiettiva**, definita come il limite proiettivo dei quozienti G/N con N che varia fra i sottogruppi normali di G (la chiusura proiettiva di $\mathbb{Z}$ è infatti $\hat{\mathbb{Z}}$).

Osservazione. Definisco $\mathbb{Q}^{ab} = \bigcup_{\substack{K \supseteq \mathbb{Q} \\ \text{abel. fin.}}} K$ la massima sottoestensione di $\overline{\mathbb{Q}}$ abeliana su $\mathbb{Q}$; $\mathbb{Q}^{ab}$ è fissata dal minimo sottogruppo chiuso N di $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tale che G/N sia abeliano, cioè $N = \overline{[G,G]}$. G/N non è altro che l'abelianizzato di G.

Proposizione 2.4.3. *L'abelianizzato di G è isomorfo a $\hat{\mathbb{Z}}^*$.*

Dimostrazione. Per il teorema di Kronecker-Weber, $\mathbb{Q}^{ab} = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\zeta_n)$, dunque l'insieme delle estensioni ciclotomiche è filtrante nell'insieme delle sottoestensioni di $\mathbb{Q}^{ab}$, da cui:

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim \mathbb{Q}(\zeta_n)/\mathbb{Q} \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^* \cong \hat{\mathbb{Z}}^*,$$

in quanto $\{a_i\} \in \hat{\mathbb{Z}}$ è invertibile $\iff$ ciascun a_i è invertibile. □

Vogliamo adesso dimostrare che tutti i gruppi simmetrici si realizzano come gruppi di Galois su $\mathbb{Q}$; per farlo vediamo prima che tali gruppi si realizzano come gruppo di Galois su un qualche altro campo.

Sia K un campo, $T_1, \ldots, T_n$ indeterminate, $L = K(T_1, \ldots, T_n)$. Allora $\mathcal{S}_n$ agisce su L per permutazione delle indeterminate:

$$\mathcal{S}_n \ni \sigma \longmapsto \left\{ \begin{array}{c} T_1 \mapsto T_{\sigma(1)} \\ \vdots \\ T_n \mapsto T_{\sigma(n)} \end{array} \right\} \in \mathrm{Aut}(L).$$

$\mathcal{S}_n$ fissa il campo $F = L^{\mathcal{S}_n}$, e visto che è finito, abbiamo che L/F è di Galois e $\mathrm{Gal}(L/F) \cong \mathcal{S}_n$. A questo punto, preso G un gruppo finito, per il teorema di immersione di Cayley $\exists n$ tale che $G \hookrightarrow \mathcal{S}_n$, quindi L/L^G è di Galois e $\mathrm{Gal}(L/L^G) \cong G$.

Osservazione. $F = L^{\mathcal{S}_n}$ è il campo delle funzioni simmetriche; in particolare contengono le funzioni simmetriche elementari: $s_0 = 1$, $s_1 = \sum_{i=1}^n T_i$, $s_2 = \sum_{i<j} T_iT_j, \ldots$, $s_n = \prod_{i=1}^n T_i$. Dunque $K(s_1, \ldots, s_n) \subseteq F$.

Teorema 2.4.4. *1. $F = K(s_1, \ldots, s_n)$ e quindi $\mathrm{Gal}(K(T_1, \ldots, T_n)/K(s_1, \ldots, s_n)) \cong \mathcal{S}_n$.*

2. $s_1, \ldots, s_n$ sono algebricamente indipendenti.

Dimostrazione. 1. $K(s_1, \ldots, s_n) \subseteq F$, dunque $[L : K(s_1, \ldots, s_n)] \geq n!$. Ma il polinomio $p(x) = \prod_i (x - T_i) = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n \in K(s_1, \ldots, s_n)[x]$ e L è il campo di spezzamento di p su $K(s_1, \ldots, s_n)$, quindi $[L : K(s_1, \ldots, s_n)] \leq n!$.

2. Siano $S_1, \dots, S_n$ altre indeterminate e sia $f(x) = \sum_i (-1)^i S_i x^i$; allora, se $t_1, \dots, t_n$ sono le radici di f in una chiusura algebrica, $\widetilde{L} = K(S_1, \dots, S_n)(t_1, \dots, t_n) = K(t_1, \dots, t_n)$, in quanto le S_i sono le funzioni simmetriche in t_i.
   Definisco un omomorfismo di valutazione:

$$\begin{array}{ccc} K[T_1, \dots, T_n] & \longrightarrow & K[t_1, \dots, t_n] \\ T_i & \longmapsto & t_i \end{array}$$

   che è ben definito in quanto le T_i sono algebricamente indipendenti. Ma tramite questa mappa $s_i \mapsto S_i$ e le S_i sono algebricamente indipendenti, quindi anche le s_i devono esserlo. □

Osservazione. Abbiamo visto che, partendo da $T_1, \dots, T_n$ indeterminate e dette $s_1, \dots, s_n$ le funzioni simmetriche elementari nelle T_i, allora $\mathrm{Gal}(K(T_1, \dots, T_n)/K(s_1, \dots, s_n)) \cong \mathcal{S}_n$.
Viceversa, partendo da $S_1, \dots, S_n$ indeterminate e dette $t_1, \dots, t_n$ le radici del polinomio $\sum_i (-1)^i S_i x^i$, allora $\mathrm{Gal}(K(t_1, \dots, t_n)/K(S_1, \dots, S_n)) \cong \mathcal{S}_n$, in quanto $K(s_1, \dots, s_n) \cong K(S_1, \dots, S_n)$ e $K(T_1, \dots, T_n) \cong K(t_1, \dots, t_n)$.

Enunciamo il seguente importante teorema, che usiamo per trasferire la realizzabilità dei gruppi finiti da un campo generico a $\mathbb{Q}$, ma che non dimostriamo:

Teorema 2.4.5 (di irriducibilità di Hilbert)**.** *Sia $r \geq 1$ e $f(T_1, \dots, T_n, X_1, \dots, X_r) \in \mathbb{Q}[T_1, \dots, T_n, X_1, \dots, X_r]$ un polinomio irriducibile. Allora esistono infinite n-uple $(a_1, \dots, a_n) \in \mathbb{Q}^n$ tali che $f(a_1, \dots, a_n, X_1, \dots, X_r)$ sia irriducibile in $\mathbb{Q}[X_1, \dots, X_r]$.*

Corollario 2.4.6. *I gruppi simmetrici si realizzano come gruppi di Galois su $\mathbb{Q}$, cioè $\forall n \in \mathbb{N}$, esiste un campo $K \supseteq \mathbb{Q}$ tale che $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_n$.*

Dimostrazione. $\mathbb{Q}(T_1, \dots, T_n)/\mathbb{Q}(s_1, \dots, s_n)$ è finita e di caratteristica 0, quindi è semplice, cioè $\mathbb{Q}(T_1, \dots, T_n) = \mathbb{Q}(s_1, \dots, s_n)(\alpha(T_1, \dots, T_n))$, con $\alpha(T_1, \dots, T_n) = c_1 T_1 + \dots + c_n T_n \in \mathbb{Q}[T_1, \dots, T_n]$ per il teorema dell'elemento primitivo.
Sia $\mu = \mu_{\alpha(T_1, \dots, T_n)} \in \mathbb{Q}[s_1, \dots, s_n, x]$ il polinomio minimo di $\alpha(T_1, \dots, T_n)$ su $\mathbb{Q}(s_1, \dots, s_n)$ (in realtá a priori si avrebbe che $\mu \in \mathbb{Q}(s_1, \dots, s_n)[x]$, ma si puó dimostrare con un lemma tecnico che in effetti $\mu \in \mathbb{Q}[s_1, \dots, s_n][x]$); si ha che:

$$\mu(T_1, \dots, T_n, x) = \prod_{\sigma \in \mathcal{S}_n} (x - \alpha(T_{\sigma(1)}, \dots, T_{\sigma(n)})),$$

in quanto il gruppo di Galois di $\mathbb{Q}(T_1, \dots, T_n)/\mathbb{Q}(s_1, \dots, s_n)$ è $\mathcal{S}_n$ che agisce per permutazione sulle indeterminate.
$s_1, \dots, s_n$ sono algebricamente indipendenti, quindi posso applicare il teorema di irriducibilità di Hilbert: esiste una n-upla $(a_1, \dots, a_n) \in \mathbb{Q}^n$ tale che $\overline{\mu} = \mu(a_1, \dots, a_n, x)$ è irriducibile in $\mathbb{Q}[x]$. Sia $\overline{\alpha} \in \overline{\mathbb{Q}}$ radice di $\overline{\mu}$; dico che $\mathbb{Q}(\overline{\alpha})/\mathbb{Q}$ è di Galois con gruppo di Galois isomorfo a $\mathcal{S}_n$.
$\overline{\mu}$ ha grado $n!$ perché μ ha grado $n!$ nella variabile x, dunque $[\mathbb{Q}(\overline{\alpha}) : \mathbb{Q}] = n!$; d'altra parte, se $p(x) = x^n - a_1 x^{n-1} + \dots + (-1)^n a_n$ e $t_1, \dots, t_n \in \overline{\mathbb{Q}}$ sono le radici di p, allora $\overline{\alpha} = \alpha(t_1, \dots, t_n)$ (in quanto le a_i sono le funzioni simmetriche nelle t_i, le s_i sono le funzioni simmetriche nelle T_i e a_i è stato sostituito nella s_i), quindi $[\mathbb{Q}(\overline{\alpha}) : \mathbb{Q}] \leq [\mathbb{Q}(t_1, \dots, t_n) : \mathbb{Q}] \leq n!$, poiché p ha grado n.
Si conclude che $\mathbb{Q}(\overline{\alpha}) = \mathbb{Q}(t_1, \dots, t_n)$ e, visto che $\mathrm{Gal}(\mathbb{Q}(t_1, \dots, t_n)/\mathbb{Q}) < \mathcal{S}_n$ e $[\mathbb{Q}(t_1, \dots, t_n) : \mathbb{Q}] = n!$, si giunge alla tesi. □

2.5 Discriminante, traccia e norma

Cominciamo la sezione con qualche breve richiamo sul risultante.

Definizione 2.5.1. Si definisce **risultante** fra due polinomi $f(x) = \sum_{i=1}^{n} a_i x^i$ e $g(x) = \sum_{j=1}^{m} b_j x^j$ il determinante della **matrice di Sylvester**:

$$\mathrm{Ris}(f,g) = \det \mathrm{Syl}(f,g) = \det \begin{pmatrix} a_n & \dots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_n & \dots & a_0 \\ b_m & \dots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_m & \dots & b_0 \end{pmatrix}.$$

Proposizione 2.5.1. *1.* $\mathrm{Ris}(f,g) = 0 \iff (f,g) \neq 1$.

2. $\mathrm{Ris}(f,g) \in \mathbb{Z}[a_i, b_j]$ *ed è omogeneo.*

3. $\exists h, k \in \mathbb{Z}[a_i, b_j][x]$ *con* $\deg h < \deg g$ *e* $\deg k < \deg f$ *tali che* $\mathrm{Ris}(f,g) = fh + gk$.

4. $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$, $g(x) = b\prod_{j=1}^{m}(x-\beta_i)$. *Allora:*

$$\mathrm{Ris}(f,g) = a^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b^n \prod_{j=1}^{m} f(\beta_j) = a^m b^n \prod_{i,j}(\alpha_i - \beta_j).$$

Corollario 2.5.2. *Siano* $\mu_\alpha(x)$ *e* $\mu_\beta(x)$ *polinomi in cui si annullano rispettivamente* α *e* β. *Allora:*

1. $\mathrm{Ris}_y(\mu_\alpha(y), \mu_\beta(x+y))$ *si annulla in* $\alpha - \beta$.

2. $\mathrm{Ris}_y\left(\mu_{\frac{1}{\alpha}}(y), \mu_\beta(xy)\right)$ *si annulla in* $\alpha\beta$.

Definizione 2.5.2. $f \in K[x]$, $\deg f \geq 1$, $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$. Si definisce **discriminante** di f il numero:

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

Proposizione 2.5.3. $\mathrm{Ris}(f,f') = (-1)^{\binom{n}{2}} a \,\mathrm{disc}(f)$.

Dimostrazione. $f'(x) = a\sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j)$, dunque:

$$\mathrm{Ris}(f,f') = a^{n-1}\prod_{i=1}^{n} f'(\alpha_i) = a^{n-1}\prod_{i=1}^{n}\left(a\prod_{j\neq i}(\alpha_i - \alpha_j)\right).$$

□

Esempi. • $f(x) = ax^2 + bx + c$.

$$\mathrm{Ris}(f,f') = \det\begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} = -a\Delta,$$

quindi $\mathrm{disc}(f) = \Delta = b^2 - 4ac$.

- $f(x) = x^3 + ax + b$.

$$\mathrm{Ris}(f, f') = \det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix} = 4a^3 + 27b^2,$$

  quindi $\mathrm{disc}(f) = -4a^3 - 27b^2$.

Osservazione. $\mathrm{disc}(f) \in \mathbb{Z}[\text{coefficienti di } f]$, poiché $\mathrm{Ris}(f, f') \in \mathbb{Z}[\text{coefficienti di } f]$ e $a \mid \mathrm{Ris}(f, f')$ perché divide la prima colonna della matrice di Sylvester.
Inoltre $\mathrm{disc}(f) = 0 \iff \mathrm{Ris}(f, f') = 0 \iff (f, f') \neq 1 \iff f$ ha fattori multipli.

Riprendiamo la notazione $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$ e poniamo $\delta = \prod_{i<j}(\alpha_i - \alpha_j) \in K(\alpha_1, \ldots, \alpha_n)$.
Abbiamo che $\mathrm{disc}(f) = a^{2(n-1)}\delta^2 \in K$, ma in quali casi $\delta \in K$?
$K(\alpha_1, \ldots, \alpha_n)$ è il campo di spezzamento di f su K e $\mathrm{Gal}(K(\alpha_1, \ldots, \alpha_n)/K) < \mathcal{S}_n$, dunque $\mathcal{S}_n$ agisce per permutazione sugli α_i:

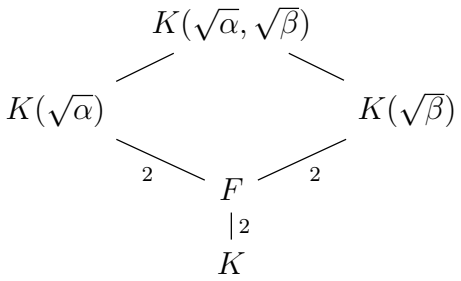
$$\begin{array}{ccc} \mathcal{S}_n & \longrightarrow & \mathcal{S}(\{\alpha_1, \ldots, \alpha_n\}) \\ \sigma & \longmapsto & \left\{ \begin{array}{c} \alpha_1 \mapsto \alpha_{\sigma(1)} \\ \vdots \\ \alpha_n \mapsto \alpha_{\sigma(n)} \end{array} \right\} \end{array}$$

Restringendo l'azione a $\{\pm\delta\}$, è immediato vedere che le permutazioni pari agiscono banalmente su δ, mentre quelle dispari mandano δ in $-\delta$; dunque abbiamo mostrato:

Proposizione 2.5.4. *$f \in K[x]$ irriducibile, $\deg f = n$, $L = K(\alpha_1, \ldots, \alpha_n)$ campo di spezzamento di f su K. Allora $\mathrm{Gal}(L/K) \subseteq \mathcal{A}_n \iff \delta \in K \iff \mathrm{disc}(f) \in K^2$.*

Esempio (Polinomi cubici). Se $f \in K[x]$ è irriducibile e $\deg f = 3$, allora, posto F il campo di spezzamento di f su K, $\mathrm{Gal}(F/K) < \mathcal{S}_3$ e dunque è o $\mathcal{S}_3$ o $\mathcal{A}_3 = \mathbb{Z}/3\mathbb{Z}$.
Per quanto appena visto, $\mathrm{Gal}(F/K) \cong \mathbb{Z}/3\mathbb{Z} \iff \mathrm{disc}(f) \in K^2$.

Esempio (Polinomi biquadratici). $\mathrm{char}(K) \neq 2$, $f(x) = x^4 + ax^2 + b \in K[x]$ irriducibile, L campo di spezzamento di f su K. Vista la limitazione sulla caratteristica del campo, f è separabile. Vediamo che tipo di isomorfismo ha $\mathrm{Gal}(L/K) < \mathcal{S}_4$.
Poniamo $g(x) = x^2 + ax + b$; detto $\Delta = a^2 - 4b$, siano α, β le radici di g in K. Allora $f(x) = (x^2 - \alpha)(x^2 - \beta)$ e quindi $L = K(\sqrt{\alpha}, \sqrt{\beta})$ è il campo di spezzamento di f su K. Denotato $F = K(\sqrt{\Delta}) = K(\alpha) = K(\beta)$, si ha un diagramma:



e $[K(\sqrt{\alpha}) : F] = [K(\sqrt{\beta}) : F] = 2$ in quanto se fosse 1 si avrebbe che $x^2 - \alpha$ (e dunque f) non sarebbe irriducibile.
Dunque $[L : K] = 4$ o 8. $[L : K] = 4 \iff K(\sqrt{\alpha}) = K(\sqrt{\beta}) \iff F(\sqrt{\alpha}) = F(\sqrt{\beta}) \iff \sqrt{\alpha} = n + m\sqrt{\beta} \iff \sqrt{\alpha} = m\sqrt{\beta} \iff F \ni \alpha = m\sqrt{\alpha\beta} \iff \alpha\beta = b \in F^2$, quindi se

$b \notin F^2$, $[L:K] = 8$ e quindi $\mathrm{Gal}(L/K)$ è il 2-Sylow di $\mathcal{S}_4$, cioè $\mathrm{Gal}(L/K) \cong D_4$.
Se invece $b \in F^2$, allora $b = (c + d\sqrt{\Delta})^2 = c^2 + d^2\Delta + 2cd\sqrt{\Delta} \in F^2 \Rightarrow cd = 0$; se $c = 0$, allora $b = d^2\Delta \notin K^2$, in quanto $\Delta \notin K^2$, mentre se $c \neq 0$ (e quindi $d = 0$), allora $b = c^2 \in K^2$. Visto che:

$$\mathrm{disc}(f) = \prod_{i<j}(x_i - x_j)^2 = \cdots = (4\alpha)(4\beta)(\alpha-\beta)^4 = 16\underbrace{\alpha\beta}_{=b}\underbrace{(\alpha-\beta)}_{=\pm\sqrt{\Delta}}^4 = 16b\Delta^2,$$

allora $\mathrm{disc}(f) \in K^2 \iff b \in K^2$; ne segue che:

- se $b \in K^2$, $\mathrm{Gal}(L/K) \subseteq \mathcal{A}_4$ e dunque $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- se $b \notin K^2$, $\mathrm{Gal}(L/K) \not\subseteq \mathcal{A}_4$ e dunque $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$ (in quanto l'unico sottogruppo transitivo di $\mathcal{S}_4$ isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ é contenuto dentro $\mathcal{A}_4$).

Definizione 2.5.3. G gruppo, K campo. Un **carattere** è un omomorfismo $\chi : G \to K^*$.

Osservazione. L'insieme dei caratteri non è chiuso rispetto alla somma, ma può essere visto come un sottoinsieme del K-spazio vettoriale degli omomorfismi K-lineari $G \to K$.

Teorema 2.5.5 (di indipendenza dei caratteri di Artin)**.** *Caratteri distinti sono linearmente indipendenti.*

Dimostrazione. Sia n il minimo tale che $\exists \chi_1, \ldots \chi_n$ distinti e linearmente dipendenti, $n \geq 2$. Allora esistono $a_1, \ldots, a_n \in K$ tali che $a_1\chi_1 + \ldots + a_n\chi_n \equiv 0$.
Ma preso $h \in G$ tale che $\chi_1(h) \neq \chi_2(h)$, si ha:

$$\begin{cases} a_1\chi_1(h)\chi_1(g) + \ldots + a_n\chi_1(h)\chi_n(g) = 0 \\ a_1\chi_1(h)\chi_1(g) + \ldots + a_n\chi_n(h)\chi_n(g) = 0 \end{cases}$$

da cui sottraendo si ottiene una combinazione lineare di lunghezza $< n$ non nulla che dà l'omomorfismo nullo, in contraddizione con la minimalità di n. □

Definizione 2.5.4. $\varphi : V \to W$ K-lineare. Definisco $\det\varphi$ come $\det A$ e $\mathrm{Tr}\,\varphi$ come $\mathrm{tr}\,A$, dove A è la matrice associata a φ rispetto a una qualunque base.

Definizione 2.5.5. L/K finita, $\alpha \in L$, $\varphi_\alpha : L \to L$ moltiplicazione per α. Si definiscono **traccia** e **norma** di α:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}\,\varphi_\alpha \qquad \mathrm{N}_{L/K}(\alpha) = \det\varphi_\alpha.$$

Osservazioni. 1. $\mathrm{Tr}_{L/K}(\alpha), \mathrm{N}_{L/K}(\alpha) \in K$.

2. $\mathrm{Tr}_{L/K}(a\alpha + b\beta) = a\,\mathrm{Tr}_{L/K}(\alpha) + b\,\mathrm{Tr}_{L/K}(\beta)$ $\forall a, b \in K$, $\forall \alpha, \beta \in L$.
3. $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$ $\forall \alpha, \beta \in L$.
4. $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = \|z\|^2$.

Lemma 2.5.6. $[L:K] = n$.

1. *$\alpha \in K$. Allora $\mathrm{Tr}_{L/K}(\alpha) = n\alpha$, $\mathrm{N}_{L/K}(\alpha) = \alpha^n$.*
2. *Se $L = K(\alpha)$ e $\mu_\alpha(x) = x^n + c_1x^{n-1} + \ldots + c_n$, allora $\mathrm{Tr}_{L/K}(\alpha) = -c_1$ e $\mathrm{N}_{L/K}(\alpha) = (-1)^n c_n$.*

3. $\alpha \in L$, $[L : K(\alpha)] = s$. *Allora* $\mathrm{Tr}_{L/K}(\alpha) = s\,\mathrm{Tr}_{K(\alpha)/K}(\alpha)$ *e* $\mathrm{N}_{L/K}(\alpha) = \big(\mathrm{N}_{K(\alpha)/K}(\alpha)\big)^s$.

Dimostrazione. Rispettivamente basta notare che $\varphi_\alpha = \alpha\,\mathrm{Id}$, μ_α è il polinomio caratteristico di $[\varphi_\alpha]$, e il polinomio caratteristico di $[\varphi_\alpha]$ è $(\mu_\alpha(x))^s$. □

Proposizione 2.5.7. $n = [L : K] = [L : K]_i[L : K]_s = q \cdot r$, $\sigma_1, \ldots, \sigma_r$ *immersioni di* L/K. *Allora* $\forall \alpha \in L$:

$$\mathrm{Tr}_{L/K}(\alpha) = q \sum_{i=1}^{r} \sigma_i(\alpha), \qquad \mathrm{N}_{L/K}(\alpha) = \left(\prod_{i=1}^{r} \sigma_i(\alpha) \right)^q.$$

Dimostrazione. Se $\alpha \in K$ la tesi è banale. Sia invece α tale che $L = K(\alpha)$; abbiamo:

$$\mu_\alpha(x) = x^n + c_1 x^{n-1} + \ldots + c_n = \prod_{i=1}^{r} (x - \sigma_i(\alpha))^q = \left(x^r - \sum_{i=1}^{r} \sigma_i(\alpha) x^{r-1} + \ldots + (-1)^r \prod_{i=1}^{r} \sigma_i(\alpha) \right)^q,$$

dunque usando il punto 2) del lemma precedente si ricava la tesi.
Infine, se $\alpha \in L$ generico, con $[L : K(\alpha)] = s = q_1 \cdot r_1$, $[K(\alpha) : K] = q_2 \cdot r_2$, $r = r_1 \cdot r_2$, $q = q_1 \cdot q_2$, allora per il punto 3) del lemma:

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)]\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) = (q_1 r_1) q_2 \sum_{i=1}^{r_2} \tau_i(\alpha),$$

con le τ_i immersioni di $K(\alpha)/K$.
Ma ogni τ_i si estende in r_1 modi a L che si comportano come τ_i su α, dunque:

$$\mathrm{Tr}_{L/K}(\alpha) = (q_1 q_2) r_1 \sum_{i=1}^{r_2} \tau_i(\alpha) = q \sum_{i=1}^{r} \sigma_i(\alpha).$$

Per la norma il ragionamento è del tutto analogo. □

Corollario 2.5.8. L/K *normale. Allora* $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L/K}(\sigma(\alpha))$ *e* $\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{L/K}(\sigma(\alpha))$ $\forall \sigma \in \mathrm{Aut}_K(L)$.

Corollario 2.5.9. $K \subseteq L \subseteq M$. *Allora* $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ *e* $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$.

Dimostrazione. Basta notare che, dopo aver spezzato il grado separabile da quello inseparabile, se γ_i sono le immersioni di L/K e τ_j sono le immersioni di M/L allora le immersioni di M/K sono $\widetilde{\gamma_i} \circ \tau_j$, dove $\widetilde{\gamma_i}$ è un'estensione qualsiasi di γ_i a M. □

Corollario 2.5.10. L/K *finita.*

1. L/K *è separabile* $\iff$ $\mathrm{Tr}_{L/K}$ *è non banale* $\iff$ *è surgettiva.*
2. *Se* L/K *è separabile, l'applicazione bilineare:*

$$\begin{array}{rccc} \mathrm{tr}: & L \times L & \longrightarrow & L \\ & (x, y) & \longmapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

è non degenere e induce un isomorfismo:

$$\begin{array}{rccc} \varphi: & L & \longrightarrow & \widehat{L} \\ & x & \longmapsto & \mathrm{Tr}_{L/K}(x\bullet) \end{array}$$

Dimostrazione. 1. $\Leftarrow$) Se L/K non è separabile, la traccia è identicamente 0 perché $q = [L : K]_i$ è una potenza della caratteristica.

$\Rightarrow$) Restringendo le immersioni $\sigma_i : L^* \to \overline{K}^*$, la traccia è somma di caratteri e dunque non identicamente nulla.

2. $\mathrm{Ker}(\varphi) = \{x \mid \mathrm{Tr}_{L/K}(xL) = 0\} = \{x \mid xL = 0\} = \{0\}$ e si conclude per dimensione.

□

<u>*Osservazione*</u>. $\widehat{L} = \varphi(L) = \{\mathrm{Tr}_{L/K}(x\bullet)\}_{x\in L}$, dunque se $\{x_1, \ldots, x_n\}$ è una K-base di L, si ha una **base duale** $\{y_1, \ldots, y_n\}$ K-base di L tale che:

$$\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}.$$

Infatti esiste $\{f_1, \ldots, f_n\}$ K-base di $\widehat{L}$ tale che $f_j(x_i) = \delta_{ij}$, ma φ è surgettiva e dunque esistono $y_1, \ldots, y_n$ tali che $f_i = \mathrm{Tr}_{L/K}(y_i\bullet)$ $\forall i$; $\{y_1, \ldots, y_n\}$ è una K-base di L in quanto la sua immagine tramite φ è una base di $\widehat{L}$.

Proposizione 2.5.11. *$L = K(\alpha)$ separabile, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ K-base di L. Detto $f(x)$ il polinomio minimo di α su K, allora, se $\frac{f(x)}{x-\alpha} = \beta_{n-1}x^{n-1} + \ldots + \beta_1 x + \beta_0$, si ha che:*

$$\left\{\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}\right\}$$

è la base duale di $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Dimostrazione. Dobbiamo verificare che $\mathrm{Tr}_{L/K}\left(\frac{\beta_i}{f'(\alpha)}\alpha^m\right) = \delta_{im}$. Sia:

$$g_m(x) = \mathrm{Tr}_{L/K}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^m}{f'(\alpha)}\right) = \mathrm{Tr}_{L/K}\left(\sum_{i=0}^{n-1}\frac{\beta_i}{f'(\alpha)}x^i\alpha^m\right) = \sum_{i=0}^{n-1} x^i\,\mathrm{Tr}_{L/K}\left(\frac{\beta_i}{f'(\alpha)}\alpha^m\right).$$

Dico che $g_m(x) = x^m$ (e avrei la tesi). Per vederlo, mi basta mostrare che $g_m(x) - x^m$ ha n radici, in quanto $m \leq n-1$. Siano $\alpha_1, \ldots, \alpha_n$ radici di $f(x)$, con $\sigma_i(\alpha) = \alpha_i$ (le σ_i sono le immersioni di L/K); allora:

$$g_m(x) = \sum_{i=1}^{n}\sigma_i\left(\frac{f(x)}{x-\alpha}\frac{\alpha^m}{f'(\alpha)}\right) = \sum_{i=1}^{n}\frac{f(x)}{x-\alpha_i}\frac{\alpha_i^m}{f'(\alpha_i)},$$

dunque:

$$g_m(\alpha_l) = \sum_{i=1}^{n}\frac{f(x)}{x-\alpha_i}\bigg|_{x=\alpha_l}\frac{\alpha_i^m}{\prod_{j\neq i}(\alpha_i-\alpha_j)} = \prod_{j\neq l}(\alpha_l-\alpha_j)\frac{\alpha_l^m}{\prod_{j\neq l}(\alpha_l-\alpha_j)} = \alpha_l^m.$$

□

<u>*Osservazione*</u>. L/K separabile finita, $\{x_1, \ldots, x_n\}$ K-base di L. Se $K \subseteq F \subseteq L$, allora $\{\mathrm{Tr}_{L/F}(x_1), \ldots, \mathrm{Tr}_{L/F}(x_n)\}$ genera F/K.
Infatti se $\alpha \in F$, L/F è separabile e dunque $\exists\gamma \in L$ tale che $\mathrm{Tr}_{L/F}(\gamma) = \alpha$; se $\gamma = \sum_{i=1}^n a_i x_i$, allora $\alpha = \sum_{i=1}^n a_i\,\mathrm{Tr}_{L/F}(x_i)$.

Teorema 2.5.12 (90 di Hilbert)**.** *L/K ciclica (e dunque finita) di grado n, $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$. Allora:*

1. $\mathrm{N}_{L/K}(\alpha) = 1 \iff \exists\beta \in L^*$ *tale che* $\alpha = \frac{\beta}{\sigma(\beta)}$.
2. $\mathrm{Tr}_{L/K}(\alpha) = 0 \iff \exists\beta \in L$ *tale che* $\alpha = \beta - \sigma(\beta)$.

Dimostrazione. Osserviamo che l'implicazione $\Leftarrow$ è ovvia in entrambi i casi; vediamo dunque l'altra.

1. Sia $\alpha \in L^*$ tale che $\mathrm{N}_{L/K}(\alpha) = 1$. La somma di caratteri:

$$\chi = 1 + \alpha\sigma + \alpha\sigma(\alpha)\sigma^2 + \ldots + \left(\alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha)\right)\sigma^{n-1} \not\equiv 0,$$

dunque esiste $\gamma \in L^*$ tale che $\chi(\gamma) \neq 0$. Sia $\beta = \chi(\gamma)$; abbiamo:

$$\begin{cases} \beta = \gamma + \alpha\sigma(\gamma) + (\alpha\sigma(\alpha))\sigma^2(\gamma) + \ldots + (\alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha))\,\sigma^{n-1}(\gamma) \\ \sigma(\beta) = \sigma(\gamma) + \sigma(\alpha)\sigma^2(\gamma) + (\sigma(\alpha)\sigma^2(\alpha))\sigma^3(\gamma) + \ldots + (\sigma(\alpha)\sigma^2(\alpha)\ldots\sigma^{n-1}(\alpha))\,\sigma^n(\gamma) \end{cases}$$

Osservato che $\sigma^n(\gamma) = \gamma$ e che $1 = \mathrm{N}_{L/K}(\alpha) = \alpha\sigma(\alpha)\sigma^2(\alpha)\ldots\sigma^{n-1}(\alpha)$, è evidente che $\alpha\sigma(\beta) = \beta$.

2. Per separabilità di L/K, esiste $\gamma \in L$ tale che $\mathrm{Tr}_{L/K}(\gamma) \neq 0$. Poniamo:

$$\beta = \frac{1}{\mathrm{Tr}_{L/K}(\gamma)}\left(\alpha\sigma(\gamma) + (\alpha + \sigma(\alpha))\sigma^2(\gamma) + \ldots + (\alpha + \sigma(\alpha) + \ldots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\gamma)\right).$$

Quindi si ha:

$$\sigma(\beta) = \frac{1}{\mathrm{Tr}_{L/K}(\gamma)}\left(\sigma(\alpha)\sigma^2(\gamma) + (\sigma(\alpha) + \sigma^2(\alpha))\sigma^3(\gamma) + \ldots + \left(\sigma(\alpha) + \ldots + \sigma^{n-1}(\alpha)\right)\underbrace{\sigma^n(\gamma)}_{=\gamma}\right),$$

da cui:

$$\beta - \sigma(\beta) = \frac{1}{\mathrm{Tr}_{L/K}(\gamma)}\left(\alpha\left(\sigma(\gamma) + \sigma^2(\gamma) + \ldots + \sigma^{n-1}(\gamma)\right) - \underbrace{\left(\sigma(\alpha) + \ldots + \sigma^{n-1}(\alpha)\right)}_{=-\alpha}\right) = \alpha.$$

□

Il precedente è la versione classica del famoso teorema 90 di Hilbert; esiste però una sua formulazione più generale in termini coomologici, che implica la versione precedente; prima di enunciarla abbiamo bisogno di qualche definizione.

Sia G un gruppo e sia A un G-modulo, cioè un gruppo abeliano su cui G agisce per moltiplicazione a sinistra nel modo naturale, cioè $\varphi : G \to \mathrm{Aut}(A)$ è un'azione e $g \cdot a := \varphi_g(a)$ $\forall g \in G, a \in A$.

Definizione 2.5.6. Si definisce **primo gruppo di coomologia** di G a valori in A il quoziente:

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

dove $Z^1(G, A) = \{f : G \to A \mid f(\sigma\circ\sigma') = \sigma(f(\sigma'))f(\sigma)\ \forall \sigma, \sigma' \in G\}$ è il gruppo degli 1**-cocicli** e $B^1(G, A) = \{f : G \to A \mid \exists a \in A \text{ tale che } f(\sigma) = \sigma(a)^{-1}a\ \forall \sigma \in G\} \triangleleft Z^1(G, A)$ è il sottogruppo degli 1**-cobordi**.

Teorema 2.5.13 (90 di Hilbert - versione coomologica)**.** *L/K di Galois finita, $G = \mathrm{Gal}(L/K)$. Allora:*

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

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

Dimostrazione. 1. Sia $f : G \to L^*$ un 1-cociclo. Vediamo che è un 1-cobordo.
$\sum_{\sigma' \in G} f(\sigma')\sigma'$ è una combinazione non nulla di caratteri, dunque esiste $c \in L^*$ tale che $b = \sum_{\sigma' \in G} f(\sigma')\sigma'(c) \neq 0$. Se $\sigma \in G$:

$$\sigma(b) = \sum_{\sigma' \in G} \underbrace{\sigma(f(\sigma'))}_{=f(\sigma\circ\sigma')f(\sigma)^{-1}} (\sigma \circ \sigma')(c) = f(\sigma)^{-1} \sum_{\sigma' \in G} f(\sigma \circ \sigma')(\sigma \circ \sigma')(c) =$$
$$= f(\sigma)^{-1} \sum_{\sigma' \in G} f(\sigma')\sigma'(c) = f(\sigma)^{-1} b.$$

2. $f : G \to L$ 1-cociclo, cioè $f(\sigma \circ \sigma') = \sigma(f(\sigma')) + f(\sigma)$. Cerco b tale che $f(\sigma) = b - \sigma(b)$ $\forall \sigma \in G$.
Se c è tale che $\mathrm{Tr}_{L/K}(c) \neq 0$, dico che l'elemento:

$$b = \frac{1}{\mathrm{Tr}_{L/K}(c)} \sum_{\sigma' \in G} f(\sigma')\sigma'(c)$$

funziona; il conto conclude la dimostrazione.

□

Come avevamo annunciato, vediamo che effettivamente la versione coomologica è più forte di quella classica: sia L/K ciclica di grado n, con $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$, e sia $\alpha \in L^*$ tale che $\mathrm{N}_{L/K}(\alpha) = 1$. Definiamo:

$$\begin{array}{rccc} f: & G & \longrightarrow & L^* \\ & \sigma^i & \longmapsto & \alpha\sigma(\alpha)\dots\sigma^{i-1}(\alpha) \end{array}$$

f è un 1-cociclo, infatti:

$$f(\sigma^i \circ \sigma^j) = f(\sigma^{i+j}) = \alpha\sigma(\alpha)\dots\sigma^{\overline{i+j-1}}(\alpha) = \alpha\sigma(\alpha)\dots\sigma^{i+j-1}(\alpha),$$

(dove $\overline{k}$ indica la classe di resto di k modulo n) in quanto $\mathrm{N}_{L/K}(\alpha) = \alpha\sigma(\alpha)\dots\sigma^{n-1}(\alpha) = 1$, mentre:

$$\sigma^i(f(\sigma^j))f(\sigma^i) = \sigma^i(\alpha\sigma(\alpha)\dots\sigma^{j-1}(\alpha))\alpha\sigma(\alpha)\dots\sigma^{i-1}(\alpha) = \alpha\sigma(\alpha)\dots\sigma^{i+j-1}(\alpha).$$

Ma allora f è un 1-cobordo, dunque $\exists\beta$ tale che $\alpha = f(\sigma) = \sigma(\beta)^{-1}\beta$.

2.6 Estensioni cicliche: teoremi di Kummer e Artin-Schreier

Teorema 2.6.1 (Kummer)**.** *K campo,* $\mathrm{char}(K) \nmid n$*, $\zeta_n \in K$.*

1. *Se L/K è ciclica di grado n, allora $\exists\alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha(x) = x^n - c$.*
2. *Se $L = K(\alpha)$ e α è radice di $x^n - c \in K[x]$, allora L/K è ciclica di grado $d \mid n$. Inoltre $\mu_\alpha(x) = x^d - \alpha^d$ (in particolare $\alpha^d \in K$, e $[L : K] = \min\{d \mid \alpha^d \in K\}$).*

Dimostrazione. 1. L'estensione è ciclica, dunque $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$; visto che $\zeta_n \in K$, allora $\mathrm{N}_{L/K}(\zeta_n^{-1}) = (\zeta_n^{-1})^n = 1$.
Per il teorema 90 di Hilbert, esiste $\alpha \in L^*$ tale che $\zeta_n^{-1} = \frac{\alpha}{\sigma(\alpha)}$, cioè tale che $\sigma(\alpha) = \zeta_n\alpha$. Dunque $G\alpha = \{\zeta_n^i\alpha\}_{0\leq i\leq n-1}$.
Osservo che $\zeta_n^i\alpha \neq \zeta_n^j\alpha$ $\forall i \neq j$, in quanto il polinomio $x^n - 1$ è separabile (perché $\mathrm{char}(K) \nmid n$), dunque $\langle\zeta_n\rangle$ è ciclico di ordine n; ma allora α ha n coniugati, quindi ha grado n e perciò $L = K(\alpha)$. Inoltre $\mu_\alpha(x) = \prod_{i=0}^{n-1}(x - \zeta_n^i\alpha) = x^n - \alpha^n$.

2. Posto $f(x) = x^n - c$, sappiamo che $f(\alpha) = \alpha^n - c = 0$. Le radici di f sono $\{\zeta_n^i \alpha\}_{0 \le i \le n-1}$ e, analogamente a prima, sono tutte distinte.
Ma $\zeta_n \in K \subseteq L$, quindi tutte le radici di μ_α sono contenute in L, cioè L/K è normale; inoltre L/K è separabile, perché α è radice di un polinomio separabile, dunque L/K è di Galois. Sia $G = \mathrm{Gal}(L/K)$.
$\forall \sigma \in G$, $\sigma(\alpha) = \zeta_n^{j_\sigma} \alpha$ per un certo j_σ, ma l'omomorfismo:

$$\begin{array}{ccc} G & \longrightarrow & \langle \zeta_n \rangle \\ \sigma & \longmapsto & \zeta_n^{j_\sigma} = \frac{\sigma(\alpha)}{\alpha} \end{array}$$

è iniettivo, poiché α genera l'estensione, quindi $G \hookrightarrow \langle \zeta_n \rangle$ e perciò G è ciclico di ordine $d \mid n$.
Sia $G = \langle \sigma_0 \rangle$. Tramite l'omomorfismo precedente, $\sigma_0 \mapsto \zeta_n^{j_0} = \frac{\sigma_0(\alpha)}{\alpha}$, dunque $\sigma_0(\alpha^d) = (\sigma_0(\alpha))^d = \zeta_n^{j_0 d} \alpha^d = \alpha^d$, cioè $\alpha^d \in K$ in quanto fissato dal gruppo di Galois.
A questo punto, visto che $\mu_\alpha(x) \mid x^d - \alpha^d \in K[x]$, per motivi di grado si ha $\mu_\alpha(x) = x^d - \alpha^d$.
□

Teorema 2.6.2 (Artin-Schreier)**.** *K campo,* $\mathrm{char}(K) = p$ *primo (e dunque $\zeta_p \in K$, perché l'unica radice p-esima di 1 è 1 stesso).*

1. *Se L/K è ciclica di grado p, allora $\exists \alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha(x) = x^p - x - c$.*
2. *Se $L = K(\alpha)$ e α è radice di $x^p - x - c \in K[x]$, allora L/K è ciclica di grado 1 o p. Più precisamente, $[L : K] = 1 \iff x^p - x - c$ si spezza completamente in $K[x]$, mentre $[L : K] = p \iff x^p - x - c$ è irriducibile in $K[x]$.*

Dimostrazione. 1. Sia $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. $\mathrm{Tr}_{L/K}(1) = p = 0$, quindi per il teorema 90 di Hilbert $\exists \alpha \in L$ tale che $1 = \alpha - \sigma(\alpha)$, cioè $\sigma(\alpha) = \alpha - 1$. L'orbita di α è perciò della forma $G\alpha = \{\alpha - i\}_{0 \le i \le p-1}$, dunque α ha p coniugati, quindi $L = K(\alpha)$.
Visto che $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p - 1 - (\alpha - 1) = \alpha^p - \alpha$, allora $c = \alpha^p - \alpha \in K$ e perciò $\mu_\alpha(x) = x^p - x - c$.

2. Sia $f(x) = x^p - x - c$. $f(\alpha) = 0$, quindi anche $f(\alpha + i) = 0$ $\forall 0 \le i \le p - 1$.
$\{\alpha + i\}_{0 \le i \le p-1}$ sono le p radici distinte di f, dunque L/K è normale e separabile e cioè di Galois; sia $[L : K] = d$.

$$K \ni \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{d} (\alpha + j_i) = d\alpha + \underbrace{\sum_{i=1}^{d} j_i}_{\in K},$$

quindi $d\alpha \in K$. Se $\alpha \in K$, allora l'estensione è banale e $f(x)$ si spezza completamente in $K[x]$; se $\alpha \notin K$, allora $p \mid d$, dunque $[L : K] = d = p$ e $f(x)$ è irriducibile in $K[x]$.
□

Osservazione. In entrambi i precedenti teoremi si può evitare di usare il teorema 90 di Hilbert usando l'algebra lineare. Vediamo come separatamente:

1. G è ciclico di ordine n, dunque il polinomio caratteristico di σ è $p_\sigma(x) = x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i) \in K[x]$, dunque ζ_n è autovalore e perciò esiste $\alpha \neq 0$ tale che $\sigma(\alpha) = \zeta_n \alpha$.

2. Il polinomio caratteristico e il polinomio minimo di σ sono $p_\sigma(x) = \mu_\sigma(x) = x^p - 1 = (x-1)^p$, con $p = \mathrm{char}(K)$. Ma allora la forma di Jordan di σ è:

$$J(\sigma) = \begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

Se $v_1, \dots, v_p$ è una base di Jordan, allora $\sigma(v_1) = v_1$ (quindi $v_1 \in K$) e $\sigma(v_2) = v_2 + v_1$; ma allora $\sigma\left(\frac{1}{v_1}v_2\right) = \frac{1}{v_1}v_2 + 1$, cioè esiste α tale che $\sigma(\alpha) = \alpha + 1$.

Teorema 2.6.3 (Artin)**.** *K campo, $i \in \overline{K}$. Se $[\overline{K} : K] < +\infty$, allora $\overline{K} = K(i)$.*
Inoltre, se $\overline{K}/K$ è non banale, allora $\mathrm{char}(K) = 0$.

Dimostrazione. Sia $[\overline{K} : K] < +\infty$. Sicuramente $\overline{K}/K$ è normale e, se $\mathrm{char}(K) = 0$, è anche separabile; ma se K non fosse perfetto, allora la chiusura perfetta di K (contenuta in $\overline{K}$) avrebbe grado ∞ su K, assurdo, dunque $\overline{K}/K$ è separabile (e quindi di Galois finita) in ogni caso.
$\overline{K} \supseteq K(i)$, perciò $\overline{K}/K(i)$ è di Galois finita. Sia $G = \mathrm{Gal}(\overline{K}/K(i))$ e supponiamo per assurdo che $|G| > 1$; allora esiste l primo tale che $l \mid |G|$. Sia $H < G$ tale che $|H| = l$ e $L = \overline{K}^H$. Posto $\mathrm{char}(K) = p$, distinguiamo due casi:

$p = l$) Per Artin-Schreier esiste $a \in \overline{K}$ tale che $\overline{K} = L(a)$ e $\mu_a(x) = x^p - x - c \in L[x]$. La mappa:

$$\begin{array}{rccc} \tau: & \overline{K} & \longrightarrow & \overline{K} \\ & \alpha & \longmapsto & \alpha^p - \alpha \end{array}$$

è ovviamente surgettiva; affermo che $\mathrm{Tr}_{\overline{K}/L} \circ \tau = \tau_{|L} \circ \mathrm{Tr}_{\overline{K}/L}$. Visto che siamo in caratteristica $p > 1$:

$$\mathrm{Tr}_{\overline{K}/L}(\tau(\alpha)) = \mathrm{Tr}_{\overline{K}/L}(\alpha^p - \alpha) = \mathrm{Tr}_{\overline{K}/L}(\alpha)^p - \mathrm{Tr}_{\overline{K}/L}(\alpha) = \tau\left(\mathrm{Tr}_{\overline{K}/L}(\alpha)\right).$$

Essendo la traccia surgettiva, ne segue che anche $\tau_{|L}$ è surgettiva; in particolare esiste $\alpha \in L$ tale che $\alpha^p - \alpha - c = 0$, quindi $\mu_a(x)$ non è irriducibile, assurdo.

$p \neq l$) $\zeta_l \in L$, in quanto $[L(\zeta_l) : L] \mid l$ e $[L(\zeta_l) : L] \leq l - 1$; ma allora per il teorema di Kummer esiste $a \in \overline{K}$ tale che $\overline{K} = L(a)$ e $\mu_a(x) = x^l - c \in L[x]$. Considero $\alpha \in \overline{K}$ tale che $\alpha^l = a$; allora:

$$\mathrm{N}_{\overline{K}/L}(\alpha)^l = \mathrm{N}_{\overline{K}/L}(\alpha^l) = \mathrm{N}_{\overline{K}/L}(a) = (-1)^l(-c) = (-1)^{l+1}(c).$$

Se l è dispari, allora $\mathrm{N}_{\overline{K}/L}(\alpha)^l = c$ e dunque $\mathrm{N}_{\overline{K}/L}(\alpha) \in L$ è radice di $\mu_a(x)$, assurdo.
Se invece $l = 2$, $-c = \mathrm{N}_{\overline{K}/L}(\alpha)^2$ è un quadrato in L; ma $i \in L$, quindi c è un quadrato in L, assurdo ancora per irriducibilità di μ_a.

Concludiamo dunque che $\overline{K} = K(i)$. Vediamo adesso che se $[\overline{K} : K] = 2$, allora $\mathrm{char}(K) = 0$.
$K \subsetneq K(i) = \overline{K}$, dunque $i \notin K$ e cioè -1 non è un quadrato in K. Osserviamo però che la somma di quadrati in K è ancora un quadrato in K: se $a, b \in K$, allora $a + ib \in \overline{K}$ ed esistono $x, y \in K$ tali che $(x + iy)^2 = a + ib$, quindi:

$$\mathrm{N}_{\overline{K}/K}(a + ib) = a^2 + b^2 = (x^2 + y^2)^2 = \mathrm{N}_{\overline{K}/K}\left((x + iy)^2\right).$$

Ma allora, se $\mathrm{char}(K) = p$, $-1 = p - 1 = \sum_{i=1}^{p-1} 1$ è un quadrato, assurdo. □

Osservazione. Sia K un campo tale che $\zeta_n \in K$. Allora $\mu_\alpha(x) = x^n - c$ è irriducibile $\iff c \notin K^p \ \forall p \mid n$.
Infatti μ_α è irriducibile $\iff [K(\alpha) : K] = n \iff$ (per Kummer) $\alpha^d \notin K \ \forall d \mid n, d < n$. Ma $\alpha^d \in K \iff c = (\alpha^d)^{\frac{n}{d}} \in K^{\frac{n}{d}}$, cioè la tesi.
Osserviamo però che rimuovendo l'ipotesi $\zeta_n \in K$, l'implicazione $\Leftarrow$ diventa falsa in generale; un controesempio può essere $x^4 + 4 \in \mathbb{R}[x]$.

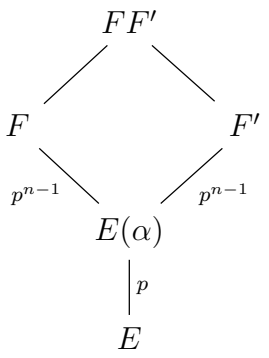
Esercizio. *Sia $\alpha \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$.*

1. *Mostrare che esiste un sottocampo massimale E di $\overline{\mathbb{Q}}/\mathbb{Q}$ che non contiene α.*
2. *Mostrare che ogni estensione finita F di E è ciclica.*
3. *Determinare* $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$.

Dimostrazione. 1. Basta applicare il lemma di Zorn all'insieme $\mathcal{F} = \{\mathbb{Q} \subseteq L \subseteq \overline{\mathbb{Q}} \mid \alpha \notin L\}$.

2. Ogni $F \supsetneq E$ contiene α per definizione di E, quindi le sovraestensioni di E hanno un elemento minimo, che è $E(\alpha)$. Se F/E è di Galois finita, $G = \mathrm{Gal}(F/E)$ ha un sottogruppo massimo $\{e\} \subsetneq H \subsetneq G$ tale che $F^H = E(\alpha)$; ma allora, se $x \in G \backslash H$, $\langle x \rangle \not\subseteq H$ e dunque $\langle x \rangle = G$ è ciclico di ordine potenza di un primo.
   Se invece F/E non è di Galois, allora $\widetilde{F}/E$ è di Galois finita, quindi è ciclica e dunque F/E è di Galois.

3. Dal punto precedente segue che $\mathrm{Gal}(E(\alpha)/E) = \mathbb{Z}/p\mathbb{Z}$ per un certo primo p; ma allora tutte le estensioni F/E hanno gruppo di Galois $\mathrm{Gal}(F/E) \cong \mathbb{Z}/p^n\mathbb{Z}$ con lo stesso p primo. Osserviamo inoltre che se $F, F'/E$ hanno grado p^n, allora il diagramma:



   mostra che $FF'/E(\alpha)$ è ciclica solamente se $F = F'$; ne segue che esiste un'unica sovraestensione di E di grado $p^n \ \forall n \geq 1$.
   Dal teorema precedente si ha che $[\overline{\mathbb{Q}} : E] \in \{2, +\infty\}$, e vale 2 solamente se E è la massima sottoestensione che non contiene i. Nel caso invece che $i \in E$, l'insieme delle sovraestensioni F/E finite è filtrante nell'insieme di tutte le sovraestensioni di E (ci deve essere un'estensione finita di grado $p^n \ \forall n$ perché $[\overline{\mathbb{Q}} : E] = +\infty$ e le estensioni finite sono cicliche), quindi:
$$\mathrm{Gal}(\overline{\mathbb{Q}}/E) = \varprojlim \mathrm{Gal}(F/E) = \mathbb{Z}_p.$$

□

Osservazione. Dall'esercizio precedente si ricava che il gruppo assoluto di Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ha tutti gli $\mathbb{Z}_p$ come sottogruppi.

2.7 Moduli di Galois: il teorema della base normale

Nel seguito sia A un anello commutativo con 1 e G un gruppo.

Definizione 2.7.1. Si definisce **anello di gruppo** l'insieme:

$$A[G] = \left\{ \sum_{g \in G} a_g g \;\middle|\; a_g \in A \text{ quasi tutti nulli} \right\}$$

con le operazioni:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g, \qquad \sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{g,h} (a_g b_h) gh.$$

Osservazione. Un $A[G]$-modulo M è un A-modulo e un G-modulo, cioè esiste un'azione $G \to \mathrm{Aut}(M)$.
In particolare, se un gruppo abeliano è un G-modulo, allora è uno $\mathbb{Z}[G]$-modulo.
Sia ora L/K estensione di Galois, $G = \mathrm{Gal}(L/K)$. É facile vedere che L è un $K[G]$-modulo. Inoltre, se $[L : K] = n < +\infty$, sia L che $K[G]$ sono K-moduli liberi di rango n; dunque, se L fosse libero anche su $K[G]$, si avrebbe necessariamente che il rango è 1. Vogliamo mostrare che effettivamente questo è vero in generale; per farlo abbiamo bisogno di qualche lemma.

Proposizione 2.7.1. *L/K finita e separabile,* $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$, $\alpha_1, \dots, \alpha_n \in L$. *$\{\alpha_1, \dots, \alpha_n\}$ è una K-base di L* $\iff \mathrm{disc}_{L/K}(\{\alpha_1, \dots, \alpha_n\}) = \det(\sigma_i(\alpha_j))^2 \neq 0$.

Dimostrazione. $\sum_{j=1}^n b_j \alpha_j = 0 \iff \sum_{j=1}^n b_j \sigma_i(\alpha_j) = 0 \ \forall i \iff$ le colonne di $(\sigma_i(\alpha_j))$ sono dipendenti. □

Lemma 2.7.2. *K campo infinito, $S \subseteq K$, $|S| = +\infty$. Allora per ogni $f \in K[x_1, \dots, x_n] \backslash \{0\}$, esistono $s_1, \dots, s_n \in S$ tali che $f(s_1, \dots, s_n) \neq 0$.*

Dimostrazione. Procediamo per induzione; il passo base $n = 1$ è evidente.
Fissiamo $n - 1$ incognite come parametri, cioè:

$$f(x_1, \dots, x_n) = \sum_{i=1}^{d} a_i(x_1, \dots, x_{n-1}) x_n^i.$$

Per ipotesi induttiva esistono $s_1, \dots, s_{n-1}$ tali che $f(s_1, \dots, s_{n-1}, x_n) \not\equiv 0$, ad esempio perché non annullano il coefficiente di grado massimo, dunque esiste $s_n \in S$ tale che $f(s_1, \dots, s_n) \neq 0$. □

Proposizione 2.7.3. *K campo infinito, L/K finita di Galois, $G = \mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Allora per ogni $f \in L[x_1, \dots, x_n] \backslash \{0\}$ esiste $\alpha \in L$ tale che $f(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \neq 0$.*

Dimostrazione. Sia $\{\alpha_1, \dots, \alpha_n\}$ una K-base di L; allora, detta $A = (\sigma_i(\alpha_j))$, dalla prima proposizione si ha $\det(A) \neq 0$. Consideriamo l'applicazione:

$$\begin{array}{rccc} \psi: & \overline{K}[x_1, \dots, x_n] & \longrightarrow & \overline{K}[y_1, \dots, y_n] \\ & f(x_1, \dots, x_n) & \longmapsto & g(y_1, \dots, y_n) = f\left(A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right) \end{array}$$

ψ è invertibile, in quanto è un cambio di base fatto tramite una matrice invertibile; dunque $g(y_1, \dots, y_n) = 0 \iff f(x_1, \dots, x_n) = 0$.
Visto che $f \not\equiv 0$ (e dunque $g \not\equiv 0$), per il lemma esistono $s_1, \dots, s_n \in K$ tali che $g(s_1, \dots, s_n) \neq 0$; ma:

$$g(s_1, \dots, s_n) = f\left(\sum_j \sigma_1(\alpha_j) s_j, \dots, \sum_j \sigma_n(\alpha_j) s_j \right) = f\left(\sigma_1\left(\sum_j \alpha_j s_j \right), \dots, \sigma_n\left(\sum_j \alpha_j s_j \right) \right),$$

cioè la tesi. □

Osservazione. Se K è finito, la proposizione precedente è falsa; se infatti $K = \mathbb{F}_q$ e $L = \mathbb{F}_{q^n}$, il polinomio $f(x_1, \ldots, x_n) = x_1^{q^n} - x_1$ si annulla su tutte le n-uple in L^n.

Teorema 2.7.4 (della base normale)**.** *L/K di Galois finita, $G = \mathrm{Gal}(L/K)$. Allora esiste $\alpha \in L$ tale che $L = K[G]\alpha$, cioè L è un $K[G]$-modulo libero di rango 1.*
Tale α si dice ***generatore della base normale****.*

Dimostrazione. Separiamo i casi $|K| < +\infty$ e $|K| = +\infty$.

$|K| < +\infty$) Supponiamo $|K| = q$; allora $\mathrm{Gal}(L/K) = \langle\phi\rangle$, con $\phi : x \mapsto x^q$ Frobenius di L. ϕ è K-lineare e $p_\phi(x) = x^n - 1$; ma per il teorema di indipendenza dei caratteri, anche $m_\phi(x) = x^n - 1 = p_\phi(x)$, dunque per un noto risultato di algebra lineare esiste una base ciclica di L/K del tipo $\{\alpha, \phi(\alpha), \ldots, \phi^{n-1}(\alpha)\}$ (per una dimostrazione di questo fatto si veda il libro *Number Theory, volume 1* di Cohen, Theorem 3.2.5).

$|K| = +\infty$) La tesi è equivalente a vedere che esiste $\alpha \in L$ tale che $\mathrm{disc}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = \det(\sigma_i(\sigma_j(\alpha)))^2 \neq 0$.
$\sigma_i \circ \sigma_j = \sigma_k$ per un certo $k = k(i,j)$, dunque considero l'applicazione:

$$\begin{array}{rccc} \varphi: & \{1,\ldots,n\} \times \{1,\ldots,n\} & \longrightarrow & \{1,\ldots,n\} \\ & (i,j) & \longmapsto & k(i,j) \end{array}$$

Le due applicazioni $\varphi(i, \bullet)$ e $\varphi(\bullet, j)$ sono evidentemente biunivoche $\forall i, \forall j$. Date $X_1, \ldots, X_n$ indeterminate, considero la matrice $B = (X_{\varphi(i,j)})_{i,j}$; per bigettività di $\varphi(i, \bullet)$ e $\varphi(\bullet, j)$, su ogni riga e su ogni colonna di B compare esattamente una e una sola X_i per ogni i.
Il determinante di B $\det(B) = d(X_1, \ldots, X_n)$ è un polinomio; tale polinomio non è identicamente nullo, in quanto $d(1, 0, \ldots, 0) = \pm 1$. Ma allora per la proposizione precedente esiste $\alpha \in L$ tale che $0 \neq d(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = \det(\sigma_{\varphi(i,j)}(\alpha)) = \det(\sigma_i(\sigma_j(\alpha)))$, che è la tesi.

□

2.8 Gruppi risolubili e risolubilità per radicali

Definizione 2.8.1. Un gruppo G si dice **risolubile** se ammette una serie normale, cioè una catena di sottogruppi:

$$G = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_n = \{e\}$$

con $G_{i+1} \triangleleft G_i$, con i quozienti $\frac{G_i}{G_{i+1}}$ abeliani.

Esempi.
- I gruppi abeliani sono risolubili.
- I p-gruppi sono risolubili (in quanto l'esistenza di una serie normale è garantita dai teoremi di Sylow e i quozienti hanno ordine p).
- I prodotti semidiretti $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/m\mathbb{Z}$ sono risolubili.

Osservazione. Se G è risolubile e finito, usando il teorema di struttura dei gruppi abeliani finiti e la corrispondenza fra sottogruppi, si può raffinare la serie normale in modo che i quozienti siano ciclici di ordine primo.

Definizione 2.8.2. Definiamo **sottogruppo dei commutatori** di G il sottogruppo $DG = [G, G] = \langle\{[g, h] = ghg^{-1}h^{-1} \mid g, h \in G\}\rangle$.

Osservazione. G è abeliano $\iff DG = \{e\}$.
Inoltre, se $N \triangleleft G$, il quoziente $\frac{G}{N}$ è abeliano $\iff N \supseteq DG$.

Definizione 2.8.3. Definiamo **sottogruppi derivati di ordine superiori** i sottogruppi D^iG, con $D^0G = G$ e ricorsivamente $D^{i+1}G = [D^iG, D^iG]$.

Osservazione. $G = D^0G \supseteq D^1G \supseteq \ldots$. Inoltre tale successione è tale che le prime k inclusioni, con $0 \leq k < +\infty$, sono strette, mentre dalla $k+1$-esima in poi sono tutte uguaglianze. Inoltre evidentemente $D^{i+1}G \triangleleft D^iG$ e $\frac{D^iG}{D^{i+1}G}$ è abeliano.

Proposizione 2.8.1. *G è risolubile $\iff D^nG = \{e\}$ per un certo $n \geq 1$.*

Dimostrazione. L'implicazione $\Leftarrow$ è del tutto ovvia; vediamo l'altra.
Sia $G = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_n = \{e\}$ una serie normale. $\frac{G_i}{G_{i+1}}$ è abeliano $\forall i$, quindi con un'immediata induzione si ha che $D^iG \subseteq G_i \ \forall i$, e perciò $D^nG \subseteq G_n = \{e\}$. □

Osservazione. $f : G \to G'$ omomorfismo. Allora $[f(g), f(h)] = f([g,h])$, dunque $Df(G) = f(DG)$.

Proposizione 2.8.2. *1. G risolubile. Allora ogni sottogruppo H di G è risolubile.*

2. $H \triangleleft G$. G è risolubile $\iff H$ e $\frac{G}{H}$ sono risolubili.

Dimostrazione. 1. Se $D^nG = \{e\}$, allora $D^nH \subseteq D^nG = \{e\}$.

2. L'implicazione $\Rightarrow$ è facile, in quanto, se $\pi : G \to \frac{G}{H}$ è la proiezione, $D^n\frac{G}{H} = D^n\pi(G) = \pi(D^nG) = \{e\}$.
Viceversa, se $D^mH = \{e\}$ e $D^n\frac{G}{H} = \{e\}$, allora $\pi(D^nG) = \{e\}$, cioè $D^nG \subseteq H$, quindi $D^mD^nG = D^{m+n}G \subseteq D^mH = \{e\}$.

□

Corollario 2.8.3. *$\prod_{i=1}^n G_i$ è risolubile $\iff G_i$ è risolubile $\forall i$.*

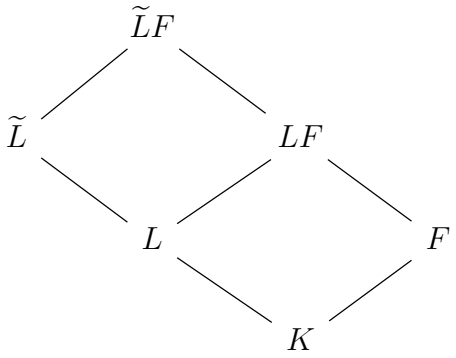
Dimostrazione. Per induzione, se $\prod_{i=1}^{n-1} G_i$ e G_n sono risolubili, allora per la proposizione precedente anche $\prod_{i=1}^n G_i$ lo è. □

Definizione 2.8.4. L/K si dice **risolubile** se esiste $E \supseteq L$ tale che E/K è di Galois e $\mathrm{Gal}(E/K)$ è risolubile.

Osservazioni.
- L/K risolubile, $K \subseteq F \subseteq L \Rightarrow F/K$ è risolubile.
- L/K risolubile è separabile.
- L/K è risolubile $\iff \mathrm{Gal}(\widetilde{L}/K)$ è risolubile.

Come abbiamo fatto ogni volta che abbiamo incontrato un tipo di estensioni, caratterizziamolo tramite le solite proprietà:

Proprietà. 2. Le estensioni risolubili si conservano nel traslato: sia L/K risolubile e $\widetilde{L}$ la chiusura normale di L/K; abbiamo il diagramma:

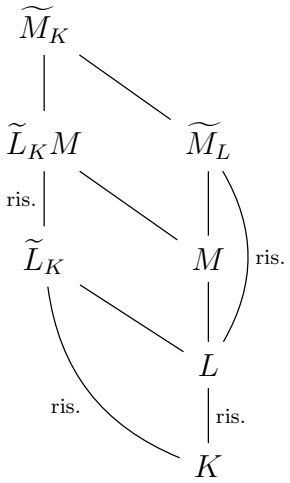


Per vedere che LF/F è risolubile, osserviamo che ci basta mostrarlo nel caso L/K di Galois con gruppo di Galois risolubile, in quanto altrimenti con la stessa dimostrazione si vede che $\widetilde{L}F/F$ è risolubile e quindi anche LF/F lo è.
In questo caso particolare, LF/F è di Galois e $\mathrm{Gal}(LF/F) < \mathrm{Gal}(L/K)$, quindi è risolubile perché sottogruppo di un gruppo risolubile.

1. Vogliamo vedere che le estensioni risolubili si conservano nelle torri, cioè, dati $K \subseteq L \subseteq M$, M/K è risolubile $\iff$ M/L e L/K sono risolubili.

   $\Rightarrow$) Ovviamente L/K è risolubile; inoltre come prima, a meno di ragionare con $\widetilde{M}$ chiusura normale di M/K, posso supporre M/K di Galois e dunque $\mathrm{Gal}(M/L) < \mathrm{Gal}(M/K)$ è risolubile.

   $\Leftarrow$) Sia $\widetilde{M}_K$ la chiusura normale di M/K, $\widetilde{L}_K$ quella di L/K e $\widetilde{M}_L$ quella di M/L; abbiamo il diagramma:



   Come prima posso supporre M/L di Galois con gruppo di Galois risolubile; posso anche supporre L/K di Galois, poiché altrimenti ragiono con $\widetilde{L}_K$ e dimostro che $\widetilde{L}_K M/K$ è risolubile (in quanto $\widetilde{L}_K M/\widetilde{L}_K$ è di Galois con gruppo di Galois risolubile perché lo è M/L), da cui anche M/K è risolubile.
   In questo caso particolare, affermo che $\mathrm{Gal}(\widetilde{M}_K/K)$ è risolubile. Per vederlo basta mostrare che lo sono $\mathrm{Gal}(L/K)$ e $\mathrm{Gal}(\widetilde{M}_K/L)$ (in quanto sono un sottogruppo e il quoziente del gruppo $\mathrm{Gal}(\widetilde{M}_K/K)$); il primo lo è per ipotesi. Per l'altro, osservo che:

$$\mathrm{Gal}(\widetilde{M}_K/L) \hookrightarrow \prod_{\sigma} \mathrm{Gal}(\sigma(M)/L),$$

   con le σ immersioni di M/L; ma visto che $\mathrm{Gal}(\sigma(M)/L) \cong \mathrm{Gal}(M/L)$ $\forall \sigma$, allora $\mathrm{Gal}(\sigma(M)/L)$ è risolubile $\forall \sigma$ e dunque anche $\mathrm{Gal}(\widetilde{M}_K/L)$ lo è.

3. Banalmente le estensioni risolubili si conservano nel composto grazie ai primi due punti.

Definizione 2.8.5. L/K finita si dice **risolubile per radicali** se esiste $E \supseteq L$ e una catena:

$$K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_n = E$$

tale che, $\forall i$, vale una delle seguenti condizioni:

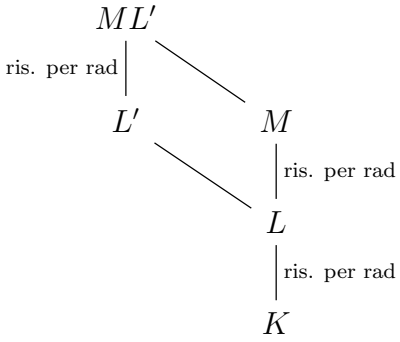
1. $E_i = E_{i-1}(\alpha)$, con α radice dell'unità;
2. $E_i = E_{i-1}(\alpha)$, con α radice di $x^n - a \in E_{i-1}[x]$, e $\mathrm{char}(K) \nmid n$;

3. $E_i = E_{i-1}(\alpha)$, con α radice di $x^p - x - c \in E_{i-1}[x]$, e $\mathrm{char}(K) = p$.

Caratterizziamo anche le estensioni risolubili per radicali tramite le proprietà:

Proprietà. 2. Le estensioni risolubili per radicali si conservano nel traslato: se infatti L/K è risolubile per radicali e F/K è un'estensione, allora esiste $E \supseteq L$ tale che $K = E_0 \subseteq \ldots \subseteq E_n = E$ con le proprietà precedenti e traslando con F si ottiene una catena $F = FE_0 \subseteq \ldots FE_n = FE$ con le proprietà precedenti tale che $FE \supseteq FL$.

1. Le estensioni risolubili per radicali si conservano nelle torri, cioè, date $K \subseteq L \subseteq M$, M/K è risolubile per radicali $\iff$ sia L/K che M/L lo sono. L'implicazione $\Rightarrow$ è ovvia, in quanto L/K è banalmente risolubile per radicali e M/L lo è perché una catena per M/K traslata con L diventa una catena per M/L.
   Per l'altra implicazione, sia $K = L_0 \subseteq \ldots \subseteq L'$, $L' \supseteq L$, una catena per L/K; si ha il diagramma:

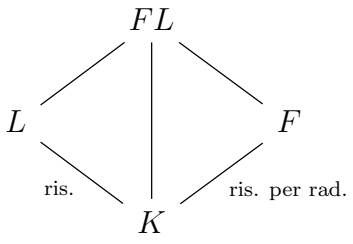


   in quanto le estensioni risolubili per radicali si conservano nel traslato. Prolungando la catena precedente con una catena per ML'/L' si ottiene una catena per ML'/K, quindi ML'/K è risolubile per radicali e dunque lo è anche M/K.

3. Le estensioni risolubili per radicali si conservano nel composto grazie ai primi due punti.

Teorema 2.8.4. *L/K finita. L/K è risolubile $\iff$ è risolubile per radicali.*

Dimostrazione. $\Rightarrow$) Come al solito posso supporre L/K di Galois con gruppo di Galois risolubile. Sia $m = \prod_{\substack{p \mid [L:K] \\ p \neq \mathrm{char}(K)}} p$; considero $F = K(\zeta_m)$. Abbiamo il diagramma:

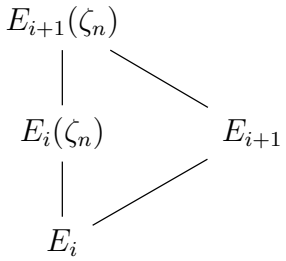


Per mostrare che L/K è risolubile per radicali, basta vedere che lo è FL/K, dunque basta vedere che lo è FL/F. L/K è di Galois risolubile, quindi FL/F è di Galois risolubile, $G = \mathrm{Gal}(LF/F)$. G ammette una serie normale $G = G_0 \supsetneq G_1 \supsetneq \ldots \supsetneq G_n = \{e\}$ con quozienti ciclici di ordine primo; passando alla catena dei sottocampi si ha:

$$F \subsetneq F_1 \subsetneq \ldots \subsetneq F_n = LF,$$

con $\frac{F_i}{F_{i-1}}$ di Galois ciclica di ordine p_i.
Se $[F_i : F_{i-1}] = p_i \mid m$, in F ci sono le radici p_i-esime dell'unità, dunque per Kummer $F_i = F_{i-1}(\alpha)$ con α radice di $x^n - a \in F_{i-1}[x]$; se invece $[F_i : F_{i-1}] = p \nmid m$, allora $[F_i : F_{i-1}] = p = \mathrm{char}(K)$ e si ha la tesi per Artin-Schreier.

$\Leftarrow$) L/K è risolubile per radicali, quindi esiste una catena $K = E_0 \subseteq \ldots \subseteq E_n = E$ con le solite proprietà. Posso supporre $E = L$, poiché se vedo che E/K è risolubile, lo è anche L/K. Ma E/K è risolubile $\iff$ E_{i+1}/E_i è risolubile $\forall i$, quindi supponiamo $E_{i+1} = E_i(\alpha)$. Se α è una radice dell'unità o una radice di $x^p - x - c \in E_i[x]$ con $p = \mathrm{char}(K)$, allora l'estensione è abeliana o ciclica e dunque risolubile. Se invece α è radice di $x^n - a \in E_i[x]$, consideriamo il diagramma:



$E_i(\zeta_n)/E_i$ è risolubile, $E_{i+1}(\zeta_n) = E_i(\zeta_n)(\alpha)/E_i(\zeta_n)$ è risolubile per Kummer, dunque $E_{i+1}(\zeta_n)/E_i$ è risolubile, perciò anche E_{i+1}/E_i lo è.

□

Osservazione. Un polinomio $p(x) \in K[x]$ ammette soluzioni scritte utilizzando solo le 4 operazioni e l'estrazione di radice se e solo se, detto L il campo di spezzamento di p su K, l'estensione L/K è risolubile per radicali.
Segue dunque il noto teorema:

Teorema 2.8.5 (Abel-Ruffini)**.** *L'equazione generale di grado n è risolubile per radicali* $\iff$ $n \leq 4$.

Dimostrazione. Dalla precedente proposizione e dall'osservazione, si ha che l'equazione generale di grado n è risolubile per radicali $\iff$ il suo campo di spezzamento ha gruppo di Galois risolubile, cioè se e solo se $\mathcal{S}_n$ è risolubile, cosa che vale $\iff$ $n \leq 4$. □

Nel seguito della sezione, dati $a, b \in \mathbb{F}_p$, $a \neq 0$, denotiamo:

$$\begin{array}{rccc} \sigma_{a,b}: & \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ & x & \longmapsto & ax + b \end{array}$$

Il sottogruppo $F_p = \{\sigma_{a,b}\}_{a,b} < \mathcal{S}(\mathbb{F}_p)$ si chiama **sottogruppo lineare**; evidentemente $|F_p| = p(p-1)$.

Definizione 2.8.6. $G < \mathcal{S}_p$ si dice **lineare** se esiste una bigezione $\phi : \{1, \ldots, p\} \to \mathbb{F}_p$ grazie alla quale $G \hookrightarrow F_p$.

Sia $\pi \in \mathcal{S}_p$ un p-ciclo; indichiamo con $N_{\mathcal{S}_p}(\pi)$ il suo normalizzatore in $\mathcal{S}_p$.

Proposizione 2.8.6. $N_{\mathcal{S}_p}(\pi) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^*$.

Dimostrazione. Detto $N = N_{\mathcal{S}_p}(\pi)$, sicuramente $\langle\pi\rangle \triangleleft N$ e $\langle\pi\rangle \cong \mathbb{Z}/p\mathbb{Z}$. N agisce su $\{1, \ldots, p\}$, quindi:

$$|\operatorname{orb}_N(1)| \cdot |\operatorname{Stab}_N(1)| = |N|,$$

ma π permuta tutti gli elementi, dunque $|\operatorname{orb}_N(1)| = p$ e $|\operatorname{Stab}_N(1)| = p - 1$.
$\langle\pi\rangle \cap \operatorname{Stab}_N(1) = \{e\}$ perché π non stabilizza 1, dunque:

$$N \cong \langle\pi\rangle \rtimes \operatorname{Stab}_N(1).$$

A questo punto, preso $\sigma \in \mathrm{Stab}_N(1)$, sicuramente $\sigma\pi\sigma^{-1} = \pi^r$, dunque a meno di isomorfismo possiamo supporre $\pi = (1\ \dots\ p)$ e $r+1 = \pi^r(1) = \sigma\pi\sigma^{-1}(1) = \sigma(\pi(1)) = \sigma(2)$, da cui:

$$\begin{array}{ccc} \mathrm{Stab}_N(1) & \longrightarrow & \mathbb{Z}/p\mathbb{Z}^* \\ \sigma & \longmapsto & r = \sigma(2) - 1 \end{array}$$

è l'isomorfismo cercato. □

<u>*Osservazione*</u>. F_p e $N_{\mathcal{S}_p}(\pi)$ sono isomorfi.

Proposizione 2.8.7. *Se $\sigma \in F_p$ ha almeno due punti fissi, allora è l'identità.*

Dimostrazione. L'equazione $ax + b = x$ ha una e una sola soluzione se $a \neq 1$, mentre se $a = 1$ ne ha almeno una se e solo se $b = 0$. □

Lemma 2.8.8. *Sia $G < \mathcal{S}_p$ un gruppo risolubile che agisce transitivamente su $\{1, \dots, p\}$. Allora G ha un unico sottogruppo di ordine p.*

Dimostrazione. Consideriamo una catena discendente:

$$G = G_0 \supsetneq G_1 \supsetneq \dots \supsetneq G_n = \{e\}$$

con quozienti ciclici di ordine primo. L'orbita di 1 tramite G ha cardinalità p, dunque $p \mid |G|$; denotiamo $p_i = \left|\frac{G_i}{G_{i-1}}\right|$. Vediamo per induzione su i che G_i agisce transitivamente su $\{1, \dots, p\}$ $\forall i < n$; il caso $i = 0$ è ovvio.
Supponiamo che G_{i-1}, $i < n$, agisca transitivamente su $\{1, \dots, p\}$; siano $B_1, \dots, B_r$ le orbite dell'azione di G_i su $\{1, \dots, p\}$, con $B_i = \mathrm{orb}(x_i)$. Dalla formula delle classi $|B_j| = \frac{|G_i|}{|\mathrm{Stab}_{G_i}(x_j)|}$ e ovviamente $p = \sum_{j=1}^{n} |B_j|$.
Dati $x, y \in \{1, \dots, p\}$, esiste $g \in G_{i-1}$ tale che $g(x) = y$; visto che $gG_ig^{-1} = G_i$ in quanto $G_i \triangleleft G_{i-1}$ e che:

$$\mathrm{Stab}_{G_i}(y) = g^{-1}\,\mathrm{Stab}_{gG_ig^{-1}}(x)g,$$

si ottiene che $|\mathrm{Stab}_{G_i}(x)| = |\mathrm{Stab}_{G_i}(y)|$. Ma allora $|B_i| = |B_j|$ $\forall i \neq j$ e dunque $|B_i| \in \{1, p\}$. Ma $i < n$, quindi $G_i \neq \{e\}$ ed esiste pertanto un'orbita non banale.
Grazie a questo ricaviamo che G_{n-1} è ciclico di ordine p, in quanto $p \mid |G_i|$ $\forall i < n$. Sia quindi $H < G$ di cardinalità p; dico che $H = G_{n-1}$. Per vederlo, mostriamo per induzione su i che $H < G_i$ $\forall i < n$, essendo il caso $i = 0$ banale.
$H < G_{i-1}$, dunque consideriamo la composizione:

$$\begin{array}{ccccc} \langle x \rangle = H & \hookrightarrow & G_{i-1} & \longrightarrow & \frac{G_{i-1}}{G_i} \\ x & \longmapsto & x & \longmapsto & \overline{x} \end{array}$$

Se per assurdo non si avesse $\overline{x} = \overline{e}$, allora $\overline{x}$ avrebbe ordine p e dunque $p^2 \mid |G_i|$, assurdo in quanto $G_i < G$ e $|G| \mid p!$. □

Proposizione 2.8.9. *Sia $G < \mathcal{S}_p$ che agisce transitivamente su $\{1, \dots, p\}$. Allora sono equivalenti:*

1. *G è lineare (cioè $G \subseteq N_{\mathcal{S}_p}(\pi)$ per un certo p-ciclo π);*
2. *G è risolubile.*

Dimostrazione. Visto che l'implicazione 1) ⇒ 2) è ovvia, vediamo l'altra.
Visto che l'azione è transitiva, $p \mid |G|$ e dunque $\pi \in G$ per un certo p-ciclo π; per il lemma $\langle \pi \rangle$ è l'unico sottogruppo di G di cardinalità p e dunque $\langle \pi \rangle \triangleleft G$, cioè $G \subseteq N_{\mathcal{S}_p}(\pi)$. □

Vediamo adesso come questa teoria si applica allo studio di alcune estensioni di Galois.

Proposizione 2.8.10. *$f \in K[x]$ irriducibile e separabile di grado p, $G = \mathrm{Gal}(L/K)$, con L campo di spezzamento di f su K. Se G è risolubile, allora $L = K(\alpha, \beta)$, dove α, β sono due qualsiasi radici di f.*

Dimostrazione. Sicuramente $K \subseteq K(\alpha,\beta) \subseteq L$; sia $H < G$ che fissa $K(\alpha,\beta)$.
G agisce transitivamente su $\{1,\dots,p\}$ per irriducibilità di f, dunque per la proposizione precedente G è lineare, ma gli elementi di $H \subseteq G$ fissano sia α che β, da cui $H = \{e\}$. □

Corollario 2.8.11. *Se f di grado p è irriducibile su $\mathbb{Q}$ e ha almeno due radici reali e una non reale, allora il gruppo di Galois di f su $\mathbb{Q}$ non è risolubile.*

Sia $f \in K[x]$ monico e separabile di grado n e sia L il campo di spezzamento di f su K, $L = K(\alpha_1,\dots,\alpha_n)$. $G = \mathrm{Gal}(L/K) < \mathcal{S}(\{\alpha_1,\dots,\alpha_n\})$.

Proposizione 2.8.12. *Se $B_1,\dots,B_r$ sono le orbite di $\{\alpha_1,\dots,\alpha_n\}$ sotto l'azione di G, allora $f = f_1 \cdot \ldots \cdot f_r$ su K, dove $f_i(x) = \prod_{\alpha \in B_i}(x-\alpha)$.*

Dimostrazione. $f_i(x) \in K[x]$ perché è fissato da G; $f_1 \cdot \ldots \cdot f_r \mid f$, ma vale l'uguaglianza perché f è monico e i due polinomi hanno le stesse radici. L'irriducibilità degli f_i deriva dal fatto che gli elementi di B_i sono coniugati fra di loro. □

<u>*Osservazione*</u>. Classificati tutti i sottogruppi transitivi di $\mathcal{S}_n$, stabilire chi sia $\mathrm{Gal}(L/K)$ equivale a controllare quali siano fra questi i sottogruppi che contengono permutazioni con tipo di cicli corrispondenti al tipo di fattorizzazione di f.
Se ad esempio $G = \langle\sigma\rangle$ è ciclico e $f = f_1 \cdot \ldots \cdot f_r$, σ è di tipo $d_1 + \ldots + d_r$, con $d_i = \deg(f_i)$.
Enunciamo un importante teorema che non dimostriamo, che stabilisce un ponte fra la teoria di Galois e la teoria dei numeri:

Teorema 2.8.13. *Sia A UFD, $K = K(A)$ il suo campo delle frazioni, $f \in A[x]$ monico, $P \subseteq A$ primo, e denotiamo $\overline{f} \in \frac{A}{P}[x]$ e $\overline{K} = K\left(\frac{A}{P}\right)$. Supponiamo inoltre che f e $\overline{f}$ non abbiano radici multiple. Se G_f e $G_{\overline{f}}$ sono rispettivamente i gruppi di Galois dei campi di spezzamento di f e $\overline{f}$ su K e $\overline{K}$, allora $G_{\overline{f}} < G_f$ se li vediamo entrambi come sottogruppi di $\mathcal{S}(\{\alpha_1,\dots,\alpha_n\})$ radici di f.*

<u>*Osservazione*</u>. Con gli strumenti della teoria algebrica dei numeri riusciamo a dimostrare questo teorema nel caso $A = \mathbb{Z}$, con $p \nmid \mathrm{disc}(f)$. In questo caso infatti $G_{\overline{f}}$ è ciclico generato dal Frobenius, cioè $G_{\overline{f}} = \langle\overline{\sigma}\rangle$ con $\overline{\sigma}$ permutazione di tipo $d_1 + \ldots + d_r$, dove $d_i = \deg(\overline{f_i})$ e $\overline{f} = \overline{f_1} \cdot \ldots \cdot \overline{f_r}$.
Ma preso un qualunque primo Q di L sopra p, con L campo di spezzamento di f su $\mathbb{Q}$, abbiamo:

$$G_{\overline{f}} = \langle\overline{\sigma}\rangle \cong \langle\sigma\rangle = D(Q|p) < G_f,$$

e questo non dipende dal primo sopra p, in quanto i gruppi di decomposizione $D(Q|p)$ e $D(Q'|p)$ differiscono per coniugio e non cambiano i tipi di permutazione.
Rimarrebbe solo da verificare che i tipi di permutazione in $G_{\overline{f}}$ e $D(Q|p)$ non cambiano tramite l'isomorfismo; questo però è facile in quanto si ha il diagramma:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \frac{\mathcal{O}_L}{Q} & \xrightarrow[\overline{\sigma}]{} & \frac{\mathcal{O}_L}{Q} \end{array}$$

che commuta, da cui $\overline{\sigma}(\overline{\gamma}) = \overline{\sigma(\gamma)}$ e dunque l'isomorfismo $\sigma \mapsto \overline{\sigma}$ mantiene i tipi di permutazione (infatti non modifica le orbite e $\overline{\sigma}(\overline{\alpha_i}) = \overline{\alpha_j} \iff \sigma(\alpha_i) = \alpha_j$).

Esempio. Il gruppo di Galois del polinomio $f(x) = x^5 - x - 1 \in \mathbb{Z}[x]$ su $\mathbb{Q}$ è isomorfo a $\mathcal{S}_5$ (e dunque le sue radici non sono esprimibili tramite le quattro operazioni e l'estrazione di radice). Infatti modulo 2 è $[f]_2(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$, mentre modulo 5 è irriducibile (per Artin-Schreier, in quanto non si spezza completamente in $\mathbb{F}_5[x]$). Ma allora il gruppo di Galois di $[f]_2$ su $\mathbb{F}_2$ è ciclico generato da un $2+3$-ciclo, mentre il gruppo di Galois di $[f]_5$ su $\mathbb{F}_5$ è ciclico generato da un 5-ciclo; si ricava che il gruppo di Galois di f su $\mathbb{Q}$ contiene un $2+3$-ciclo e un 5-ciclo, cioè è $\mathcal{S}_5$ (in quanto $\mathcal{S}_5$ è generato da un 5-ciclo e da un 2-ciclo, e il cubo di un $2+3$-ciclo è un 2-ciclo).

2.9 Coomologia di moduli di Galois

Sia A un G-modulo. Useremo la notazione $A^G = \{a \in A \mid g \cdot a = a \ \forall g \in G\} < A$.
Un G-modulo A si dice **banale** se $A = A^G$.

Osservazione. Siano A, B G-moduli. Se denotiamo con $\mathrm{Hom}(A, B)$ il gruppo degli omomorfismi di gruppo da A a B, possiamo dotare tale gruppo di una struttura di G-modulo con l'operazione:

$$(g \cdot f)(a) := g \cdot f(g^{-1} \cdot a).$$

Se $\mathrm{Hom}_G(A, B)$ è il gruppo degli omomorfismi di G-moduli da A a B (cioè tali che $f(g \cdot a) = g \cdot f(a)$), è immediato osservare che:

$$\mathrm{Hom}_G(A, B) = \mathrm{Hom}(A, B)^G.$$

Proposizione 2.9.1. *Sia:*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

una successione esatta corta di G-moduli. Allora la successione per restrizione:

$$0 \longrightarrow A^G \xrightarrow{\alpha_G} B^G \xrightarrow{\beta_G} C^G$$

è esatta.

Dimostrazione. La buona definizione delle restrizioni α_G e β_G è del tutto ovvia; inoltre α_G è iniettiva perché restrizione di una mappa iniettiva e $\mathrm{Im}(\alpha_G) \subseteq \mathrm{Ker}(\beta_G)$ perché $\beta_G \circ \alpha_G = 0$. D'altronde, se $y \in \mathrm{Ker}(\beta_G)$, $\exists a \in A$ tale che $y = \alpha(a)$, ma $y \in B^G$, dunque $g \cdot \alpha(a) = \alpha(g \cdot a) = \alpha(a)$ e la tesi segue per iniettività di α. □

Osservazione. In generale, però, la mappa β_G non è surgettiva. Consideriamo ad esempio la successione esatta corta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle \zeta_n \rangle & \xhookrightarrow{i} & \overline{\mathbb{Q}}^* & \xrightarrow{\beta} & \overline{\mathbb{Q}}^* & \longrightarrow & 0 \\ & & & & x & \longmapsto & x^n & & \end{array}$$

Se $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_n))$, la successione per restrizione diventa:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \langle \zeta_n \rangle & \xhookrightarrow{i} & \mathbb{Q}(\zeta_n)^* & \xrightarrow{\beta_G} & \mathbb{Q}(\zeta_n)^* \\ & & & & x & \longmapsto & x^n \end{array}$$

e in $\mathbb{Q}(\zeta_n)$ non ci sono radici n-esime di ζ_n, cioè β_G non è surgettiva.

Osservazione. Se A è un G-modulo banale, $Z^1(G, A) = \mathrm{Hom}(G, A)$ e $B^1(G, A) = 0$.

Osservazione. $H^1(G, A)$ é un G-modulo, in quanto lo é $Z^1(G, A)$ con l'operazione $(g \cdot \varphi)(\sigma) = g\varphi(g^{-1}\sigma g)$.

Proposizione 2.9.2. *Sia:*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

una successione esatta corta di G-moduli. Allora esiste una successione esatta lunga:

$$0 \longrightarrow A^G \xrightarrow{\alpha_G} B^G \xrightarrow{\beta_G} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{\alpha_1} H^1(G,B) \xrightarrow{\beta_1} H^1(G,C) \longrightarrow \dots$$

Dimostrazione. Innanzitutto vogliamo definire δ; per farlo, sia $c \in C^G$ e $b \in B$ tale che $\beta(b) = c$. Si ha:

$$\beta(\sigma \cdot b - b) = \beta(\sigma \cdot b) - \beta(b) = \sigma \cdot \beta(b) - \beta(b) = \sigma \cdot c - c = 0$$

$\forall \sigma \in G$, cioè $\sigma \cdot b - b \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)\ \forall \sigma \in G$. Visto che α è iniettiva, a meno di isomorfismo si può supporre che α sia l'inclusione e dunque $\sigma \cdot b - b \in A$; definiamo pertanto la mappa:

$$\begin{array}{rccc} f_b: & G & \longrightarrow & A \\ & \sigma & \longmapsto & \sigma \cdot b - b \end{array}$$

e definiamo $\delta(c) := f_b + B^1(G,A)$. É immediato verificare che $f_b \in Z^1(G,A)$; vediamo inoltre che $\delta(c)$ non dipende dalla scelta di b.
Se $c = \beta(b')$, $\beta(b - b') = 0$ e dunque $b - b' = a \in A$ tramite l'inclusione α; ma allora:

$$(f_b - f_{b'})(\sigma) = \sigma b - b - \sigma b' + b' = \sigma a - a,$$

cioè $f_b - f_{b'} \in B^1(G,A)$, come voluto.
Vediamo l'esattezza in C^G:

$$\delta \circ \beta_G(b) = \delta(\beta_G(b)) = \sigma b - b + B^1(G,A) = B^1(G,A);$$

viceversa, se $c \in C^G$ e $c \in \mathrm{Ker}(\delta)$, $0 = \delta(c) = f_b + B^1(G,A)$, cioè f_b è un 1-cobordo, dunque esiste $a \in A$ tale che $\sigma b - b = \sigma a - a\ \forall \sigma \in G$, cioè $b - a \in B^G$; ma $\beta_G(a) = \beta_G(\alpha_G(a)) = 0$, dunque $c = \beta_G(b) = \beta_G(b - a)$ e $b - a \in B^G$.
Definiamo a questo punto α_1 (e analogamente β_1):

$$\begin{array}{ccccc} Z^1(G,A) & \longrightarrow & Z^1(G,B) & \longrightarrow & H^1(G,B) \\ f & \longmapsto & \alpha \circ f & \longmapsto & \alpha \circ f + B^1(G,B) \end{array}$$

e definiamo $\alpha_1(f + B^1(G,A)) = \alpha \circ f + B^1(G,B)$; tale mappa è ben definita (cioè passa al quoziente) in quanto:

$$(\alpha \circ f_a)(\sigma) = \alpha(\sigma a - a) = \sigma\alpha(a) - \alpha(a) = f_{\alpha(a)}(\sigma).$$

Tralasciamo la verifica che $\mathrm{Ker}(\alpha_1) = \mathrm{Im}(\delta)$; la verifica dell'esattezza in $H^1(G,B)$ è del tutto analoga. □

Esempio. La successione esatta già considerata:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle \zeta_n \rangle & \xhookrightarrow{i} & \overline{\mathbb{Q}}^* & \xrightarrow{\beta} & \overline{\mathbb{Q}}^* & \longrightarrow & 0 \\ & & & & x & \longmapsto & x^n & & \end{array}$$

diventa, se $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_n))$:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \langle \zeta_n \rangle & \xhookrightarrow{i} & \mathbb{Q}(\zeta_n)^* & \xrightarrow{\beta_G} & \mathbb{Q}(\zeta_n)^* & \xrightarrow{\delta} & H^1(G, \langle \zeta_n \rangle) & \longrightarrow & H^1(G, \overline{\mathbb{Q}}^*) \longrightarrow \dots \\ & & & & x & \longmapsto & x^n & & & & \end{array}$$

ma $H^1(G, \langle\zeta_n\rangle) = \mathrm{Hom}(G, \langle\zeta_n\rangle)$ in quanto $\langle\zeta_n\rangle$ è un G-modulo banale e $H^1(G, \overline{\mathbb{Q}}^*) = 0$ per Hilbert 90 (noi abbiamo visto solo il caso di estensioni di Galois finite, ma il teorema è vero per ogni estensione di Galois); la nuova successione esatta diventa pertanto:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \langle\zeta_n\rangle & \overset{i}{\hookrightarrow} & \mathbb{Q}(\zeta_n)^* & \overset{\beta_G}{\longrightarrow} & \mathbb{Q}(\zeta_n)^* & \overset{\delta}{\longrightarrow} & \mathrm{Hom}(G, \langle\zeta_n\rangle) & \longrightarrow & 0 \\ & & & & x & \longmapsto & x^n & & & & \end{array}$$

(per vedere che δ è surgettiva potevamo anche mostrare che $H^1(\varprojlim G_i, A) = \varprojlim H^1(G_i, A)$). Con questo ricaviamo ad esempio che:

$$\mathrm{Hom}(G, \langle\zeta_n\rangle) \cong \frac{\mathbb{Q}(\zeta_n)^*}{\mathrm{Im}(\beta_G)} = \frac{\mathbb{Q}(\zeta_n)^*}{(\mathbb{Q}(\zeta_n)^*)^n}$$

ed identificando $\varphi : G \to \langle\zeta_n\rangle$ con il sottogruppo $\mathrm{Ker}(\varphi) \lhd G$ di indice $d \mid n$, abbiamo una corrispondenza fra le estensioni:

$$\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ L \\ |_d \\ \mathbb{Q}(\zeta_n) \end{array}$$

tali che $L/\mathbb{Q}(\zeta_n)$ è ciclica di grado d ed elementi in $\frac{\mathbb{Q}(\zeta_n)^*}{(\mathbb{Q}(\zeta_n)^*)^n}$.
Un esempio semplice può essere la corrispondenza fra $L = K(\sqrt[d]{a})$ e $\sqrt[d]{a} \in \frac{\mathbb{Q}(\zeta_n)^*}{(\mathbb{Q}(\zeta_n)^*)^n}$.
Osservazione. Sia G il gruppo di Galois di una certa estensione di $\mathbb{Q}$; sicuramente $\mathbb{Z}$ è un G-modulo banale. Consideriamo una risoluzione libera di $\mathbb{Z}$ fatta solo da G-moduli banali:

$$P: \quad \ldots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0;$$

$K = \mathrm{Hom}_G(P, A)$, con A G-modulo, è un complesso di catene; si può dunque considerare la successione esatta:

$$0 \longrightarrow \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0^*} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1^*} \mathrm{Hom}_G(P_2, A) \xrightarrow{d_2^*} \ldots$$

e definire **q-esimo gruppo di coomologia** di G a valori in A:

$$H^q(G, A) := H^q(K) = \frac{\mathrm{Ker}(d_q^*)}{\mathrm{Im}(d_{q-1}^*)}.$$

Si può verificare che la definizione non dipende dalla risoluzione scelta e coincide con quella data da noi precedentemente; inoltre si può dimostrare che $H^0(G, A) = A^G$ e che, data una successione esatta corta:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

esiste una successione esatta lunga (che estende quella da noi trovata):

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \ldots$$

Sia A un G-modulo, $H \lhd G$; A^H è un G-modulo, dunque esiste una mappa $G \to \mathrm{Aut}(A^H)$, ma H agisce banalmente su A^H, dunque l'azione si quozienta a un'azione $\frac{G}{H} \to \mathrm{Aut}(A^H)$.

Proposizione 2.9.3. *La **successione di inflazione e restrizione**:*

$$0 \longrightarrow H^1\left(\frac{G}{H}, A^H\right) \xrightarrow{\alpha} H^1(G,A) \xrightarrow{\beta} H^1(H,A)$$

è esatta.

Dimostrazione. Definiamo innanzitutto le mappe di inflazione e restrizione: se $\overline{f} \in Z^1\left(\frac{G}{H}, A^H\right)$, consideriamo la composizione:

$$\begin{array}{ccccc} Z^1\left(\frac{G}{H}, A^H\right) & \longrightarrow & Z^1(G,A) & \longrightarrow & H^1(G,A) \\ \overline{f} & \longmapsto & f & \longmapsto & f + B^1(G,A) \end{array}$$

dove:

$$\begin{array}{ccccccc} G & \xrightarrow{\pi} & \frac{G}{H} & \xrightarrow{\overline{f}} & A^H & \xhookrightarrow{i} & A \\ & \searrow & & & & \nearrow & \\ & & & f & & & \end{array}$$

Definiamo $\alpha\left(\overline{f} + B^1\left(\frac{G}{H}, A^H\right)\right) = f + B^1(G,A)$; è immediato constatare che tale applicazione è ben definita per passaggio al quoziente della precedente composizione. Vediamo che tale mappa di inflazione è iniettiva: sia $\overline{f} \in \mathrm{Ker}(\alpha)$, cioè $f = f_a \in B^1(G,A)$. Poiché $f = \overline{f} \circ \pi$, f è costante sulle classi laterali di H in G, cioè $f(\sigma\tau) = f(\sigma)\ \forall \tau \in H$; scegliendo $\sigma = \mathrm{id}$, si ha:

$$\sigma\tau a - a = \sigma a - a,$$

cioè $\tau a = a\ \forall \tau \in H$, cioè $a \in A^H$, dunque $\overline{f} = \overline{f}_a \in B^1\left(\frac{G}{H}, A^H\right)$.
Definiamo invece β, cioè la restrizione; presa la composizione:

$$\begin{array}{ccccc} Z^1(G,A) & \longrightarrow & Z^1(H,A) & \longrightarrow & H^1(H,A) \\ f & \longmapsto & f_{|H} & \longmapsto & f_{|H} + B^1(H,A) \end{array}$$

è immediato vedere che passa al quoziente e tale mappa quoziente è la β voluta.
Tralasciamo la verifica dell'esattezza in $H^1(G,A)$. □

2.10 Teoria di Kummer

Dato un gruppo G, diremo (impropriamente) che G ha **esponente** n se $g^n = e\ \forall g \in G$.

Definizione 2.10.1. Un'estensione L/K si dice **di Kummer** se è abeliana di esponente n finito, con $\zeta_n \in K$ e $\mathrm{char}(K) \nmid n$.

Nel seguito sarà implicito che $\zeta_n \in K$; grazie a questo è ben definita l'estensione $K(\sqrt[n]{a})$ per $a \in K$, in quanto non dipende dalla radice n-esima scelta.

Proposizione 2.10.1. *Sia $\Delta \subseteq K$. Allora $L = K(\sqrt[n]{\Delta})/K$ è abeliana di esponente n.*

Dimostrazione. É immediato vedere che L/K è di Galois, in quanto L è il campo di spezzamento su K dell'insieme di polinomi $\{x^n - a\}_{a\in\Delta}$.
Preso $a \in \Delta$, sicuramente $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ è ciclico di ordine $d \mid n$, quindi in particolare è abeliano di esponente n; ma allora, considerata l'immersione:

$$\mathrm{Gal}(L/K) \xhookrightarrow{(res_a)_{a\in\Delta}} \prod_{a\in\Delta} \mathrm{Gal}(K(\sqrt[n]{a})/K),$$

segue che anche $\mathrm{Gal}(L/K)$ è abeliano di esponente n. □

Proposizione 2.10.2. *L/K abeliana (non necessariamente finita) di esponente n. Allora $L = K(\sqrt[n]{\Delta})$, dove $\Delta = L^{*n} \cap K^*$.*

Dimostrazione. L'inclusione $K(\sqrt[n]{\Delta}) \subseteq L$ è del tutto ovvia, perché $\Delta \subseteq L^{*n}$.
Per il viceversa, visto che L è il composto di tutte le sue sottoestensioni finite (e dunque abeliane di esponente n), per il teorema di struttura dei gruppi abeliani finiti si ha che L è il composto di tutte le sue sottoestensioni cicliche (di esponente n):

$$L = \prod_{\substack{L_i/K \\ \text{ciclica}}} L_i.$$

Ma per il teorema di Kummer, $L_i = K(\sqrt[n]{a})$ per un certo $a \in K^*$; dal momento che $\sqrt[n]{a} \in L_i \subseteq L$, sicuramente $a \in L^{*n}$, cioè la tesi. □

Osservazione.

1. Se $L = K(\sqrt[n]{\Delta})$, con $\Delta \subseteq K^*$, usando in ordine le due precedenti proposizioni si ottiene che $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{L^{*n} \cap K^*})$.

2. Sia $L = K(\sqrt[n]{a})/K$ ciclica di grado esattamente n, cioè $a \notin K^{*d}\ \forall d \mid n$. Se $\alpha = \sqrt[n]{a}$, allora $\mathrm{Gal}(L/K) = \langle\sigma\rangle$, con $\sigma(\alpha) = \zeta_n\alpha$. In questo caso vale che:

$$L^{*n} \cap K^* = \bigsqcup_{i=0}^{n-1} a^i K^{*n}.$$

Dimostrazione. Sicuramente l'unione è disgiunta, perché $a \notin K^{*d}\ \forall d \mid n$; inoltre l'inclusione $\supseteq$ è ovvia.
Per l'altra, sia $b \in L^{*n} \cap K^*$. Detto $\beta = \sqrt[n]{b} \in L = K(\alpha)$, si ha:

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

per certi $b_0, \ldots, b_{n-1} \in K$. Visto che $b \in K^*$, sia β che $\sigma(\beta)$ sono radici del polinomio $x^n - b \in K[x]$, quindi $\exists 0 \leq h < n$ tale che $\sigma(\beta) = \zeta_n^h\beta$, cioè:

$$b_0 + b_1\zeta_n\alpha + \ldots + b_{n-1}\zeta_n^{n-1}\alpha^{n-1} = b_0\zeta_n^h + b_1\zeta_n^h\alpha + \ldots + b_{n-1}\zeta_n^h\alpha^{n-1}.$$

Visto che $1, \alpha, \ldots, \alpha^{n-1}$ sono linearmente indipendenti, necessariamente si deve avere $b_i(\zeta_n^h - \zeta_n^i) = 0\ \forall i$, cioè $\beta = b_h\alpha^h$ e dunque $b = \beta^n = b_h^n\alpha^{hn}$. □

3. $L = K(\sqrt[n]{a}) = K(\sqrt[n]{b}) \iff \langle aK^{*n}\rangle = \langle bK^{*n}\rangle$ come sottogruppi di $\frac{K^*}{K^{*n}}$.

Dimostrazione. Dall'osservazione precedente si ha che $K(\sqrt[n]{a}) = K(\sqrt[n]{b}) \iff \bigsqcup_{i=0}^{n-1} a^iK^{*n} = \bigsqcup_{i=0}^{n-1} b^iK^{*n}$, in quanto una implicazione è ovvia e l'altra segue dal fatto che ogni elemento di L^* può essere espresso come radice n-esima di un elemento in $\bigsqcup_{i=0}^{n-1} a^iK^{*n}$ e di un elemento in $\bigsqcup_{i=0}^{n-1} b^iK^{*n}$.
Quindi $a \in b^kK^{*n}$ per un certo $0 < k < n$ coprimo con n, in quanto le estensioni $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ hanno lo stesso grado; ma questo equivale a dire che $\langle aK^{*n}\rangle = \langle bK^{*n}\rangle$. □

Vogliamo concludere la sezione enunciando e dimostrando il noto teorema di Kummer, che caratterizza del tutto le estensioni di Kummer. Per farlo, però, abbiamo bisogno di qualche facile risultato sui caratteri, che esponiamo di seguito.

Denotiamo con G un gruppo abeliano finito, e con $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ il gruppo dei caratteri.

Lemma 2.10.3. $\widehat{G} \cong G$.

Dimostrazione. Se G è ciclico di ordine n, la tesi segue grazie all'isomorfismo:

$$\begin{array}{ccc} \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) & \xrightarrow{\sim} & \mathbb{Z}/n\mathbb{Z} \\ \chi & \longmapsto & \chi(1) \end{array}$$

e all'osservazione $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^*) \cong \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ (in quanto l'immagine di elementi di ordine d ha ordine che divide d).
Per estendere il risultato a tutti i gruppi abeliani basta notare che:

$$\mathrm{Hom}\left(\bigoplus_i \mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*\right) \cong \bigoplus_i \mathrm{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*).$$

□

Lemma 2.10.4. $\widehat{\widehat{G}} \cong G$ *canonicamente.*

Dimostrazione. Consideriamo l'omomorfismo:

$$\begin{array}{ccc} G & \longrightarrow & \widehat{\widehat{G}} = \mathrm{Hom}(\widehat{G}, \mathbb{C}^*) \\ g & \longmapsto & g := (\chi \mapsto \chi(g)) \end{array}$$

Per cardinalità, ci basta mostrare che tale mappa è iniettiva; sia dunque g tale che $\chi(g) = 1$ $\forall \chi$. Se $H = \langle g \rangle$, tutti i caratteri $\chi \in \widehat{G}$ passano al quoziente e dunque $\widehat{G} = \widehat{G/H}$; per motivi di cardinalità necessariamente $H = \{\mathrm{id}\}$. □

Corollario 2.10.5. *Si ottiene l'**accoppiamento di dualità**: l'applicazione:*

$$\begin{array}{ccc} G \times \widehat{G} & \longrightarrow & \mathbb{C}^* \\ (g, \chi) & \longmapsto & \chi(g) \end{array}$$

è non degenere.

Definizione 2.10.2. Dato $H < G$, definiamo il suo ortogonale:

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(h) = 1 \ \forall h \in H\}.$$

A meno di identificare $\widehat{\widehat{G}}$ con G, se $X < \widehat{G}$, il suo ortogonale risulta essere:

$$X^\perp = \{h \in G \mid \chi(h) = 1 \ \forall \chi \in X\} = \bigcap_{\chi \in X} \mathrm{Ker}(\chi).$$

Osservazioni.

1. $\chi \in H^\perp \iff H \subseteq \mathrm{Ker}(\chi)$.
2. $H^\perp \cong \widehat{G/H}$ tramite la mappa $H^\perp \ni \chi \mapsto \overline{\chi} \in \widehat{G/H}$.
3. $H < G$. Allora $(H^\perp)^\perp = H$ a meno di identificazione.
   Infatti hanno la stessa cardinalità e:
   $$(H^\perp)^\perp = \{g \in G \mid \chi(g) = 1 \ \forall \chi \in H^\perp\} = \{g \in G \mid \chi(g) = 1 \ \forall H \subseteq \mathrm{Ker}(\chi)\} \supseteq H.$$
4. Dunque, a meno di identificazione, si ha una corrispondenza biunivoca:
   $$\begin{array}{ccc} \{H < G\} & \longleftrightarrow & \{X < \widehat{G}\} \\ H & \longmapsto & H^\perp \\ X^\perp & \longleftarrow & X \end{array}$$

5. Nel caso in cui $G = \mathrm{Gal}(L/K)$ abeliano finito, componendo le due corrispondenze si ha una corrispondenza biunivoca fra le sottoestensioni di L/K e i sottogruppi di $\widehat{G}$:

$$H^\perp \longleftrightarrow H \longleftrightarrow L^H.$$

   Ad esempio, tramite questa corrispondenza, $\widehat{G} \leftrightarrow L^{\{e\}} = L$.

Siamo pronti per dimostrare il teorema centrale della teoria di Kummer:

Teorema 2.10.6 (Kummer)**.** *Le estensioni abeliane di esponente n di K sono in corrispondenza biunivoca con i sottogruppi di K^* che contengono K^{*n} (e dunque in corrispondenza biunivoca con i sottogruppi di $\frac{K^*}{K^{*n}}$). Più precisamente:*

$$\begin{array}{ccc} \{L/K \text{ di Kummer}\} & \longleftrightarrow & \{\Delta < K^* \mid K^{*n} \subseteq \Delta\} \\ L & \overset{\alpha}{\longmapsto} & L^{*n} \cap K^* \\ K(\sqrt[n]{\Delta}) & \overset{\beta}{\longmapsto} & \Delta \end{array}$$

e $\alpha \circ \beta = \beta \circ \alpha = \mathrm{id}$.
Inoltre, se $L = K(\sqrt[n]{\Delta})$ con $K^{*n} \subseteq \Delta \subseteq K^*$, c'è un isomorfismo canonico:

$$\begin{array}{rccc} \psi: & \frac{\Delta}{K^{*n}} & \longrightarrow & \mathrm{Hom}_{cont}\left(\mathrm{Gal}(L/K), \langle\zeta_n\rangle\right) \\ & aK^{*n} & \longmapsto & \left(\chi_a : \begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \langle\zeta_n\rangle \\ \sigma & \mapsto & \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array}\right) \end{array}$$

Dimostrazione. Vediamo prima la seconda parte: innanzitutto osserviamo che, visto che L/K è abeliana di esponente n, $\Delta = L^{*n} \cap K^*$. Consideriamo la mappa:

$$\begin{array}{rccc} \widetilde{\psi}: & \Delta & \longrightarrow & \mathrm{Hom}_{cont}(G, \langle\zeta_n\rangle) \\ & a & \longmapsto & \chi_a \end{array}$$

Vediamo che $\widetilde{\psi}$ è ben definita, cioè che χ_a è un omomorfismo continuo; visto che $G = \mathrm{Gal}(L/K)$ è un gruppo topologico, basta vedere che $\chi_a^{-1}(1)$ è aperto in G. Ma:

$$\chi_a^{-1}(1) = \{\sigma \in G \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\} = \mathrm{Gal}(L/K(\sqrt[n]{a})),$$

che è aperto in quanto chiuso e di indice finito.
Tralasciando la banale verifica che $\widetilde{\psi}$ è un omomorfismo, osserviamo che:

$$\mathrm{Ker}(\widetilde{\psi}) = \{a \in \Delta \mid \chi_a(\sigma) = 1\ \forall \sigma \in G\} = \{a \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\ \forall \sigma \in G\} = \{a \mid \sqrt[n]{a} \in L^G = K\} = K^{*n};$$

quindi $\widetilde{\psi}$ si quozienta a ψ, che per quanto appena detto è iniettiva.
Per provare la surgettività di ψ, consideriamo come primo caso G finito. Visto che diamo ai gruppi finiti la topologia discreta, tutti gli omomorfismi $G \to \langle\zeta_a\rangle$ sono continui; dunque $\mathrm{Hom}_{cont}(G, \langle\zeta_n\rangle) = \mathrm{Hom}(G, \langle\zeta_n\rangle) = Z^1(G, \langle\zeta_n\rangle)$, in quanto $\langle\zeta_n\rangle$ è un G-modulo banale.
Per Hilbert 90, $H^1(G, L^*) = 1$, ma, essendo G di esponente n, $H^1(G, \langle\zeta_n\rangle) \subseteq H^1(G, L^*)$, dunque:

$$\mathrm{Hom}_{cont}(G, \langle\zeta_n\rangle) = Z^1(G, \langle\zeta_n\rangle) = B^1(G, \langle\zeta_n\rangle) \subseteq B^1(G, L^*) = \{\chi_b \mid b \in L^* \text{ e } \chi_b(\sigma) = \sigma(b)b^{-1}\ \forall \sigma \in G\}.$$

Per vedere la surgettività di ψ, basta mostrare che $b = \sqrt[n]{a}$ per un certo $a \in \Delta$: questo è facile perché $\left(\frac{\sigma(b)}{b}\right)^n = 1$, cioè $\sigma(b^n) = b^n$, per tutti i $\sigma \in G$ e dunque $b^n \in L^{*n} \cap K^*$.
Sia adesso L/K generica; L è composto di tutte le sue sottoestensioni finite, cioè:

$$L = \prod_{\substack{L_i/K \\ \text{finita}}} L_i.$$

Per il primo caso appena visto, $L_i = K(\sqrt[n]{\Delta_i})$ e $\frac{\Delta_i}{K^{*n}} \cong \mathrm{Hom}(\mathrm{Gal}(L_i/K), \langle\zeta_n\rangle)$; sia $\chi \in \mathrm{Hom}_{cont}(G, \langle\zeta_n\rangle)$. $\mathrm{Ker}(\chi) = \chi^{-1}(1)$ è un intorno aperto di 1 in G, ma i $\{\mathrm{Gal}(L/L_i)\}_i$ formano una base di intorni aperti di 1 in G, dunque $\mathrm{Gal}(L/L_i) \subseteq \mathrm{Ker}(\chi)$ per un certo i e χ passa al quoziente; consideriamo il diagramma:

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \langle\zeta_n\rangle \\ {\scriptstyle res}\swarrow & \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\chi}} \\ \mathrm{Gal}(L_i/K) & \xleftrightarrow{\sim} & \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/L_i)} \end{array}$$

A meno di isomorfismo, $\overline{\chi} \in \mathrm{Hom}(\mathrm{Gal}(L_i/K), \langle\zeta_n\rangle)$, dunque per il primo caso $\overline{\chi} = \chi_a$ per un certo $a \in \Delta$. Preso $\sigma \in G$, si ha:

$$\chi(\sigma) = \overline{\chi}(\sigma_{|L_i}) = \chi_a(\sigma_{|L_i}) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \chi_a(\sigma),$$

cioè $\chi = \chi_a$.
Vediamo invece la prima parte; per una proposizione precedente si ha facilmente:

$$(\beta \circ \alpha)(L) = \beta(L^{*n} \cap K^*) = K(\sqrt[n]{L^{*n} \cap K^*}) = L.$$

Per vedere che anche $\alpha \circ \beta = \mathrm{id}$, denotiamo innanzitutto:

$$\alpha \circ \beta(\Delta) = \alpha(\underbrace{K(\sqrt[n]{\Delta})}_{=L}) = L^{*n} \cap K^* =: \Delta';$$

è immediato vedere che $\Delta \subseteq \Delta'$.
Per vedere l'uguaglianza, sfruttiamo l'isomorfismo canonico trovato nella prima parte della dimostrazione; in particolare, chiamato:

$$X = \psi\left(\frac{\Delta'}{K^{*n}}\right) = \{\chi_a \mid a \in \Delta\},$$

per ottenere la tesi ci basta provare che $X = \psi\left(\frac{\Delta}{K^{*n}}\right) = \widehat{G}$ (per iniettività di ψ).
Vediamolo prima se L/K è finita; $X < \widehat{G}$ e il suo ortogonale è:

$$H = X^\perp = \bigcap_{a \in \Delta} \mathrm{Ker}(\chi_a).$$

$|G| = |X| \cdot |X^\perp| = |X| \cdot |H|$, dunque $X = \widehat{G} \iff H = \{e\}$; ma:

$$H = \{\sigma \in \mathrm{Gal}(L/K) \mid \chi_a(\sigma) = 1 \ \forall a \in \Delta\} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \ \forall a \in \Delta\},$$

da cui $H = \{e\}$, in quanto L è generata da $\{\sqrt[n]{a}\}_{a \in \Delta}$.
Nel caso generale, scriviamo Δ come unione di tutti i suoi sottogruppi finiti:

$$\Delta = \bigcup_{\substack{\Delta_i < \Delta \\ |\Delta_i| < +\infty}} \Delta_i;$$

se denotiamo $L = K(\sqrt[n]{\Delta})$ e $L_i = K(\sqrt[n]{\Delta_i})$, si vede facilmente che $L = \prod_i L_i$. Ma per quanto abbiamo visto:

$$\Delta \subseteq \Delta' = L^{*n} \cap K^* = \left(\bigcup L_i^{*n}\right) \cap K^* = \bigcup (L_i^{*n} \cap K^*) = \bigcup \Delta_i' = \bigcup \Delta_i = \Delta,$$

cioè la tesi. □

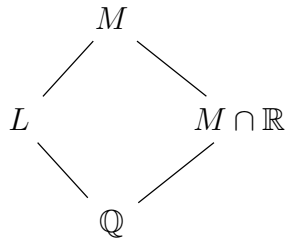
Corollario 2.10.7. *$K(\sqrt[n]{K^*})$ è la massima estensione abeliana di K di esponente n.*

Esempio. $\mathbb{Q}(\sqrt{\mathbb{Q}^*}) = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo o } p = -1\})$ è la massima estensione abeliana di $\mathbb{Q}$ di esponente 2.

Concludiamo con un teorema (che non dimostriamo) che in un certo senso generalizza la teoria di Kummer:

Teorema 2.10.8 (Albert)**.** *K campo, p primo tale che* $\mathrm{char}(K) \nmid p$ *e tale che $\zeta_{p^e} \in K$ per un certo $e \geq 1$; sia L/K ciclica di grado p^r, $r \geq 0$. Allora esiste una sovraestensione M/K di L ciclica di grado $[M : K] = p^{e+r}$ $\iff$ esiste $y \in L^*$ tale che $\mathrm{N}_{L/K}(y) = \zeta_{p^e}$.*
In tal caso, esiste $z \in L^*$ tale che $M = L(\sqrt[p^e]{z})$ e $y = \frac{\tau(\sqrt[p]{z})}{\sqrt[p]{z}}$ per un certo τ tale che $\mathrm{Gal}(M/K) = \langle\tau\rangle$.

Esempi. Consideriamo il caso $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-a})$, con $a \in \mathbb{N}$. Non è difficile osservare che non può esistere una sovraestensione M di L ciclica di grado 4 (o di grado 2^n con $n \geq 2$), in quanto altrimenti si avrebbe un diagramma:



e dunque $M/\mathbb{Q}$ avrebbe gruppo di Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
In effetti, però, notiamo che, nelle notazioni del teorema, non esiste un elemento $y \in L^*$ di norma $\zeta_{p^e} = \zeta_2 = -1$:

$$\mathrm{N}_{L/K}(x + \sqrt{-a}y) = x^2 + ay^2 \neq -1,$$

e dunque questo esempio "giustifica" il teorema di Albert.
Se invece $L = \mathbb{Q}(\sqrt{2})$, l'elemento $y = 1 + \sqrt{2}$ ha norma -1 e dunque esiste una sovraestensione di L ciclica di grado 4 su $\mathbb{Q}$. Per trovarla, cerco $z = a + b\sqrt{2}$ tale che:

$$1 + \sqrt{2} = \frac{\tau(\sqrt{z})}{\sqrt{z}}, \quad \text{cioè} \quad 3 + 2\sqrt{2} = \frac{\tau(z)}{z} = \frac{a - b\sqrt{2}}{a + b\sqrt{2}}.$$

Un facile calcolo mostra che $z = 2 - \sqrt{2}$ va bene e dunque $M = \mathbb{Q}\left(\sqrt{2 - \sqrt{2}}\right)$ è una sovraestensione di L ciclica di grado 4 su $\mathbb{Q}$.

Osservazione. Il teorema, nel caso $r = 0$, è completamente dimostrato dalla teoria di Kummer; invece, se $\zeta_{p^{e+r}} \in K$, L/K è di Kummer e corrisponde a un certo $\Delta < K^*$, $K^{*n} \subseteq \Delta$, dunque esiste una sovraestensione $M \supseteq L$ ciclica su K se esiste $\Delta \subseteq \Gamma \subseteq K^*$ tale che $\frac{\Gamma}{K^{*n}} \cong \mathrm{Gal}(M/K)$ è ciclico.