UNIVERSITÀ DI PISA

UNIVERSITÁ DI PISA
DIPARTIMENTO DI MATEMATICA
Corso di Laurea in Matematica

Appunti del corso

Teoria dei campi e teoria di Galois

A cura di:
Vincenzo Galgano
Carlo Sircana

Titolare del corso:
Prof.ssa **Ilaria Del Corso**

Indice

Introduzione

I seguenti sono appunti del corso di *Teoria dei campi e teoria di Galois* tenuto dalla Prof.ssa Del Corso nell' a.a. 2015/2016. Si danno per buoni i risultati di algebra lineare e teoria dei gruppi, mentre saranno richiamate (dove necessario) nozioni di topologia generale e di teoria dei moduli; tuttavia la conoscenza di queste ultime non é un prerequisito per il corso. La teoria viene esposta nello stesso ordine visto a lezione, mentre gli esercizi sono stati accorpati alla teoria cui fanno riferimento. I libri adottati dal docente sono *Algebra* di S. Bosch e *Algebra* di S. Lang. Per segnalazioni o altro, potete scriverci su `galgano@mail.dm.unipi.it` o `sircana@mail.dm.unipi.it` .

Revisione a cura di Jessica Alessandrì.

Capitolo 1

Estensioni di campi

1.1 Estensioni finite ed estensioni algebriche

In questa prima parte, ci occuperemo di studiare le proporietà di base delle estensioni di campi. La prima distinzione fondamentale è la seguente:

Definizione 1.1. Siano $K \subset F$ campi. Un elemento $\alpha \in F$ si dice **algebrico** su K se esiste un polinomio $p(x) \in K[x] \setminus \{0\}$ tale che $p(\alpha) = 0$. Un elemento $T \in F$ si dice **trascendente** su K se per ogni $p(x) \in K[x] \setminus \{0\}$ si ha $p(T) \neq 0$.

Per esempio, $\sqrt{2}$ è algebrico su $\mathbb{Q}$ mentre $x \in \mathbb{Q}(x)$ (il campo delle funzioni razionali a coefficienti in $\mathbb{Q}$) è trascendente.

Definizione 1.2. Un'estensione di campi F/K é detta **finita** se F ha dimensione finita come spazio vettoriale su K. Un'estensione di campi F/K é detta **algebrica** se ogni elemento $\alpha \in F$ è algebrico su K.

Valgono i seguenti risultati (che non dimostriamo in quanto dati per buoni dal corso di Algebra 1): dati $K \subset E \subset F$ campi, allora

- $E/K,\ F/E$ finite $\implies F/K$ finita;
- $E/K\ ,\ F/E$ algebriche $\implies F/K$ algebrica;
- E/K finita $\implies E/K$ algebrica.

Definizione 1.3. Siano $K \subset F$ campi e sia S un sottoinsieme di F. Definiamo

$$K(S) = \bigcup_{S_f \subset S \text{ finito}} K(S_f)$$

Osservazione. $K(S)$ é il piú piccolo sottocampo di F contenente sia K che S.

$$K(S) = \bigcap_{K, S \subset E \subset F} E$$

Definizione 1.4. Siano $E, F \subset L$ campi. Il **composto** di E ed F è il campo

$$EF = \bigcap_{E,F \subset K \subset L} K = E(F) = F(E)$$

Sappiamo che un'estensione finita é sempre algebrica, ma il viceversa é falso: basta pensare alla chiusura algebrica di $\mathbb{Q}$ o a $\mathbb{Q}(\{\sqrt[n]{2}\}_n)$.
Inoltre, poiché per definizione, un'estensione F/K é finita se $\dim_K F$ é finita, non sempre un'estensione finitamente generata é finita: basta considerare $K(T)$ con T elemento trascendente su K. Vale il seguente:

Proposizione 1.5. *Sia $F = K(a_1 \dots a_n)$ un'estensione di campi finitamente generata di K con a_i algebrici su K. Allora F/K é un'estensione finita.*

Dimostrazione. Preliminarmente, mostriamo che un'estensione semplice algebrica $L(\alpha)/L$ è finita. Sia μ_α un polinomio di $L[x]$ che si annulla in α. Detto $n = \deg(\mu_\alpha)$, si ha che $1, \dots, \alpha^{n-1}$ generano $L(\alpha)$ su L e dunque $L(\alpha)/L$ è finita. Dimostriamo allora la proposizione. Dato che gli a_i sono algebrici su K, si ha che $\forall i \leq n$ l'estensione $K(a_1 \dots a_{i-1})(a_i)/K(a_1 \dots a_{i-1})$ é un'estensione semplice e algebrica e dunque finita di campi. Ne segue che F/K è finita poiché per le estensioni finite vale la proprietá delle torri. □

Proposizione 1.6. *Siano $K \subset F$ campi e sia S un sottoinsieme di F. Se ogni $\alpha \in S$ è algebrico su K, allora $K(S)/K$ è estensione algebrica.*

Dimostrazione. Sia $\gamma \in K(S)$. Per definizione di $K(S)$ esiste $\{\alpha_1 \dots \alpha_n\} \subset S$ tale che $\gamma \in K(\alpha_1 \dots \alpha_n)$. Per ipotesi, gli α_i sono algebrici su K. Per la proposizione precedente, $K(\alpha_1 \dots \alpha_n)/K$ é finita, dunque algebrica, dunque γ é algebrico su K. Poiché ciò vale per ogni $\gamma \in K(S)$, si ha la tesi. □

Notiamo che $\mathbb{Z}$ ammette sempre un omomorfismo φ su K, ottenuto mandando $1 \mapsto 1$. Dato che un sottoanello di un campo è un dominio, si possono verificare due casi:

- Se φ è iniettivo, allora K contiene il campo dei quozienti di $\mathbb{Z}$, ossia $\mathbb{Q}$.
- Se $\ker(\varphi) = (p)$, allora $\mathbb{F}_p \subseteq K$.

Nel primo caso diciamo che la caratteristica del campo è 0 ($\mathrm{char}(K) = 0$), nel secondo che la caratteristica del campo è p ($\mathrm{char}(K) = p$).

Estensioni quadratiche L'esempio più facile di estensioni sono le estensioni quadratiche, ossia le estensioni di grado 2 (ossia L è uno spazio vettoriale di dimensione 2 su K). Data allora una base $(1, \alpha)$ di L su K, ogni estensione quadratica F/K con $\mathrm{char}(K) \neq 2$ é del tipo $F = K(\alpha) = K(\sqrt{\Delta})$. Infatti, α soddisfa un polinomio di grado 2 su K e dato che $\mathrm{char}(K) \neq 2$ possiamo utilizzare la formula risolutiva per le equazioni di secondo grado. Detto Δ il discriminante, si ha che $\sqrt{\Delta}$ genera l'estensione, perché $\sqrt{\Delta} \notin K$.

Proposizione 1.7. *Dato K campo con* $\operatorname{char} K \neq 2$*,*

$$K(\sqrt{a}) = K(\sqrt{b}) \iff \frac{a}{b} \text{ é un quadrato in } K$$

Dimostrazione. Basta notare che

$$\begin{aligned} K(\sqrt{a}) = K(\sqrt{b}) &\iff \sqrt{b} \in K(\sqrt{a}) \\ &\iff \sqrt{b} = x + y\sqrt{a} \\ &\iff b - x^2 - ay^2 - 2xy\sqrt{a} = 0 \\ &\iff xy = 0 \end{aligned}$$

Se $y = 0$, allora $\sqrt{b} \in K$, da cui un assurdo. Se invece $x = 0$, si ha $\sqrt{b} = y\sqrt{a}$, ossia $b = y^2 a$. □

Dalla proposizione precedente, deduciamo che $K^\times/(K^\times)^2$ parametrizza le estensioni di grado 2, ossia abbiamo che la mappa

$$\Phi \colon {}^{K^\times}\!/_{(K^\times)^2} \longrightarrow \{L \mid K \subset L \,, [L : K] = 2\}$$

non dipende dai rappresentanti ed è surgettiva.

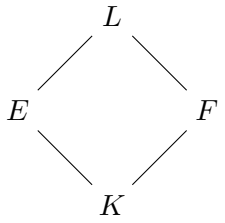
Continuiamo ora la nostra trattazione sulle estensioni di campi. Siamo interessati a studiare le estensioni algebriche, in quanto queste hanno un comportamento meno caotico delle estensioni trascendenti. In particolare, data un'estensione di campi, possiamo sempre separare una parte algebrica e una trascendente:

Definizione 1.8. Sia L/K un'estensione di campi. Definiamo la **chiusura algebrica** di K in L come l'insieme

$$\overline{K} = \{\alpha \in L \mid \alpha \text{ algebrico } su \ K\}$$

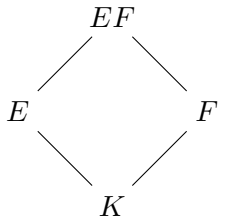
Si verifica facilmente che la chiusura algebrica è un campo. Inoltre, $\overline{K}$ è la più grande sottoestensione algebrica di L e dunque si ha che $L/\overline{K}$ è trascendente. Nello studio delle estensioni di campi porremo particolare attenzione alla verifica (o meno) di tre proprietá, che sono:

- proprietá delle **torri**: date una proprietá $\mathcal{P}$ e una torre di estensioni di campi $K \subset F \subset L$ in cui $\mathcal{P}$ vale per due estensioni, ci chiediamo se vale anche per la terza;
- proprietá dello **shift**: dati una proprietá $\mathcal{P}$ e un diagramma di estensione di campi del tipo



in cui $\mathcal{P}$ vale per un'estensione, ci chiediamo se vale anche per l'estensione parallela;

- proprietá del **composto**: dati una proprietá $\mathcal{P}$ e un diagramma di estensione di campi del tipo

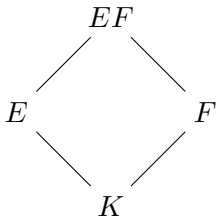


in cui $\mathcal{P}$ vale per le estensioni $K \subset E$ e $K \subset F$, ci chiediamo se vale anche per l'estensione $K \subset EF$.

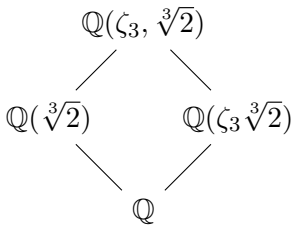
Osservazione. É evidente che se una proprietá vale per "torri" e per "shift", allora vale per "composto".

Vedendo le estensioni come spazi vettoriali e ragionando sulle basi, si dimostra che la *finitezza* delle estensioni di campi rispetta tutte e tre le proprietá di *torri*, *shift* e *composto*. Dalla relazione "finita $\implies$ algebrica" e ragionando ancora sulle basi, si verifica che le tre proprietá valgono anche per l'*algebricitá* delle estensioni.

Osservazione. Si noti che dato il diagramma



in generale vale $[EF : F] \leq [E : K]$, ma non vale $[EF : F] \nmid [E : K]$. Ad esempio, si consideri



dove $[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}(\zeta_3\sqrt[3]{2})] = 2$ ma $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Vedremo piú avanti che la condizione di divisibilitá vale sotto ipotesi piú forti.

Definizione 1.9. Un campo F si dice **algebricamente chiuso** (e lo indichiamo con $F = \overline{F}$) se ogni polinomio $f(x) \in F[x]$ di grado positivo ammette una radice in F.
Un campo F si dice **chiusura algebrica** di K (e si indica con $F = \overline{K}$) se

1. F/K é algebrica;
2. F é algebricamente chiuso.

Esistono diverse definizioni equivalenti di campo algebricamente chiuso:

- $\forall\ f(x) \in F[x]$, f si spezza completamente in fattori lineari su F;
- gli unici polinomi irriducibili sono quelli di primo grado.

Vogliamo ora dimostrare che ogni campo ammette (unica) una chiusura algebrica, ma per farlo dobbiamo prima mostrare che per ogni campo esiste un campo algebricamente chiuso che lo contiene (in modo da giustificare un ambiente in cui lavorare). Consideriamo prima il facile esempio di $\mathbb{R}$ e $\mathbb{C}$; chiaramente $\mathbb{C} = \mathbb{R}(i)$ e dunque l'estensione è algebrica. Mostriamo allora che $\mathbb{C}$ è algebricamente chiuso, ossia che $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$.

Teorema 1.10. *Il campo dei numeri complessi $\mathbb{C}$ è algebricamente chiuso.*

Dimostrazione. Sia $f \in \mathbb{C}[x]$ un polinomio di grado positivo; vogliamo mostrare che esiste $\alpha \in \mathbb{C}$ tale che $f(\alpha) = 0$. Poniamo $g(z) = |f(z)|$. La dimostrazione si sviluppa in due passi:

1. $g(z)$ ha minimo: poiché $g(z) \to \infty$ per $z \to \infty$, $\inf_{\mathbb{C}} g(z) = \inf_{|z|<R} g(z)$ e, dato che $\{|z| < R\}$ é compatto, ammette minimo

$$\inf_{z\in\mathbb{C}} g(z) = \min_{|z|<R} g(z)$$

2. Mostriamo che $\min g(z) = 0$. Procediamo per assurdo; se $\min g(x) > 0$, a meno di traslazioni e normalizzazioni, possiamo supporre $\min g(z) = 1$ e che tale minimo sia assunto in 0. Scriviamo allora $f(z) = 1 +$

$a_r z^r + ... + a_n z^n$ con $a_r \neq 0$. Valutando sulle semirette $\lambda\zeta$, al variare di $\lambda \in \mathbb{R}^+$, otteniamo

$$f(\lambda\zeta) = 1 + a_r\lambda^r\zeta^r + (\lambda\zeta)^{r+1}h(\lambda\zeta)$$

Sia η tale che $\eta^r = -a_r^{-1}$; allora $|f(\lambda\eta)| \leq |1 - \lambda^r| + |(\lambda\eta)^{r+1}h(\lambda\eta)|$. Per λ arbitrariamente piccolo,

$$\begin{aligned} |f(\lambda\eta)| &\leq 1 - \lambda^r + \lambda^{r+1}|\eta^{r+1}||h(\lambda\eta)| \\ &\leq 1 - \lambda^r(1 - \lambda|\eta^{r+1}||h(\lambda\eta)|) \\ &< 1 \end{aligned}$$

il che é assurdo poiché avevamo supposto che il minimo fosse 1.

Di conseguenza esiste $z \in \mathbb{C}$ tale che $f(z) = 0$, da cui la tesi. □

Questo mostra allora che $\mathbb{C}$ é una chiusura algebrica di $\mathbb{R}$; invece $\mathbb{C}$ non è una chiusura algebrica di $\mathbb{Q}$, in quanto in $\mathbb{C}$ ci sono elementi trascendenti su $\mathbb{Q}$. La dimostrazione più semplice di questo risultato passa da risultati sulla cardinalità di una chiusura algebrica.

L'aver dimostrato che $\mathbb{C}$ è algebricamente chiuso fornisce anche un metodo per trovare una chiusura algebrica di $\mathbb{Q}$:

Proposizione 1.11. *L'insieme*

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebrico su } \mathbb{Q}\}$$

è una chiusura algebrica di $\mathbb{Q}$.

Dimostrazione. Sappiamo che $\overline{\mathbb{Q}}$ é un campo ed é algebrico su $\mathbb{Q}$. Vediamo che $\overline{\mathbb{Q}}$ é algebricamente chiuso.
Sia $f(x) \in \overline{\mathbb{Q}}[x]$ di grado ≥ 1. Poiché $f(x) \in \mathbb{C}[x]$ e $\mathbb{C}$ é algebricamente chiuso, sappiamo che esiste $\alpha \in \mathbb{C}$ tale che $f(\alpha) = 0$. Dunque α é algebrico su $\overline{\mathbb{Q}}$ e, poiché per le estensioni algebriche vale la proprietá delle torri, α é algebrico su $\mathbb{Q}$, ossia $\alpha \in \overline{\mathbb{Q}}$.

□

Questa dimostrazione è valida per un qualsiasi campo K, purché vi sia un campo algebricamente chiuso che lo contenga. Per dimostrare l'esistenza di una chiusura algebrica, sarà allora sufficiente trovare un sovracampo algebricamente chiuso di K. Ci serve prima un lemma preliminare:

Lemma 1.12. *Siano* $f_1, ..., f_n$ *polinomi in* $K[x]$. *Allora esiste un'estensione algebrica* K' *di* K *tale che* $\forall i$ f_i *ha una radice in* K'.

Dimostrazione. Procediamo per induzione sul numero di polinomi irriducibili n. Se $n = 1$, consideriamo la fattorizzazione in irriducibili $f_1 = \mu_1^{e_1} \dots \mu_s^{e_s}$ in $K[x]$. Allora $K' = K[x]/(\mu_1)$ è un campo (poiché μ_1 é irriducibile, dunque (μ_1) é ideale primo in un PID, quindi massimale) e sappiamo che la classe $\overline{x}$ di x é radice di f_1 in K'. Inoltre l'estensione K'/K è finita in quanto, detto $n = \deg(\mu_1)$, gli elementi $1, x, \dots, x^{n-1}$ formano una base di K'. Questo dimostra anche che l'estensione è algebrica.
Procediamo ora al passo induttivo. Per ipotesi induttiva esiste un'estensione F di K in cui $f_1 \dots f_{n-1}$ hanno una radice. Fattorizziamo in $F[x]$ $f_n = \gamma_1^{d_1} \dots \gamma_r^{d_r}$ (fattorizzazione in irriducibili). Allora, come prima, consideriamo il campo $F' = F[x]/(\gamma_1)$ e notiamo che F' soddisfa la tesi. □

Dimostriamo ora il teorema di esistenza per ogni campo di un'estensione algebricamente chiusa. La dimostrazione che proponiamo é quella di Emil Artin e utilizza la costruzione di Kronecker di estensioni algebriche, appena vista nel lemma precedente.

Teorema 1.13 (Esistenza di un'estensione algebricamente chiusa)**.** *Ogni campo ammette un'estensione algebricamente chiusa.*

Dimostrazione. Sia K un campo. Posto $I = \{f \in K[x] \mid \deg f \geq 1\}$, consideriamo l'insieme delle variabili formali $\mathfrak{X} = \{X_f\}_{f \in I}$ e l'anello dei polinomi $K[\mathfrak{X}]$. Notiamo che ad ogni $f \in K[x]$ abbiamo associato un $X_f \in \mathfrak{X}$. L'ideale $J = (\{f(X_f)\}_{f \in I})$ di $K[\mathfrak{X}]$ è un ideale proprio; se per assurdo non lo fosse, allora esisterebbero $f_1 \dots f_m \in J$ e $a_i \in K[\mathfrak{X}]$ tali che

$$\mathbb{1} = \sum_{i=1}^{n} a_i f_i(X_{f_i})$$

Per il lemma precedente, esisterebbe K' contenente K contenente una radice di ogni f_i. Siano esse $\alpha_1 \dots \alpha_n$; definiamo allora l'omomorfismo di valutazione $\phi\colon K[\mathfrak{X}] \longrightarrow K'$ tale che $\phi(X_{f_i}) = \alpha_i$ e 0 altrove. Applicando ϕ all'equazione sopra otteniamo

$$\mathbb{1} = \sum_{i=1}^{n} \phi(a_i) f_i(\alpha_i) = 0$$

da cui un assurdo. Dunque J é un ideale proprio di $K[\mathfrak{X}]$ e (per Zorn) esiste un massimale $\mathfrak{m}$ che lo contiene. Poniamo $L_1 = K[\mathfrak{X}]/\mathfrak{m}$ e notiamo che K s'immerge in L_1 in quanto

$$K \hookrightarrow K[\mathfrak{X}] \longrightarrow {}^{K[\mathfrak{X}]}\!/_{\mathfrak{m}} = L_1$$

e, dato $\alpha \in K$, $\overline{\alpha} \neq 0$ in L_1. Inoltre, ogni $\overline{X_f}$ é radice di $f(x)$, infatti

$$f(\overline{X_f}) = \sum_i c_i \overline{X_f}^{\,i} = \overline{\sum_i c_i X_f^i} = \overline{f(X_f)} = 0$$

Iterando tale costruzione su L_1 e via via costruendo $L_{i+1} = L_i[\mathfrak{X}]/\mathfrak{m}_\mathfrak{i}$, otteniamo una catena ascendente di campi

$$K = L_0 \subset L_1 \subset L_2 \subset ...$$

e consideriamo $L = \bigcup_i L_i$. Ovviamente L è un campo in quanto unione di una catena ascendente di campi. Vediamo che L è algebricamente chiuso: dato $g(x) \in L[x]$, esiste i_0 tale che $g(x) \in L_{i_0}[x]$ e per costruzione $g(x)$ ha una radice in $L_{i_0+1} \subset L$. Ne segue che L é un'estensione algebricamente chiusa di K. □

Come anticipato, otteniamo il seguente corollario:

Corollario 1.14. *Ogni campo ammette una chiusura algebrica.*

Dimostrazione. È sufficiente ripetere la costruzione vista con $\mathbb{C}$ e $\mathbb{Q}$. □

Prima di indagare sull'unicità di tale chiusura algebrica, vediamo qualche esempio:

Esempio. Per ogni $p \in \mathbb{N}$ primo e per ogni $n \in \mathbb{N}$ sia

$$\mathbb{F}_{p^n} = \{\alpha \in \overline{K} \mid \alpha^{p^n} = \alpha\}$$

Sappiamo che esiste la chiusura algebrica $\overline{K}$; questa può essere caratterizzata come

$$\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$$

Infatti:

- $\overline{\mathbb{F}_p}$ è un campo: infatti $\{\mathbb{F}_{p^n}\}_n$ (pur non essendo una catena ascendente) é un insieme *filtrante*, ossia dati $r,\ s$ esiste t tale che $\mathbb{F}_{p^r},\ \mathbb{F}_{p^s} \subset \mathbb{F}_{p^t}$.
- $\overline{\mathbb{F}_p}$ è algebrico su $\mathbb{F}_p$: ciò è evidente dalla definizione degli $\mathbb{F}_{p^n}$.
- $\overline{\mathbb{F}_p}$ è algebricamente chiuso: infatti, dato $f \in \overline{\mathbb{F}_p}[x]$ di grado positivo, esiste n tale che $f \in \mathbb{F}_{p^n}[x]$. Allora, presa una radice $\alpha \in \overline{K}$, l'estensione $\mathbb{F}_{p^n}(\alpha) = \mathbb{F}_{p^{nd}} \subset \overline{\mathbb{F}_p}$ per qualche d, da cui la tesi.

Come preannunciato, dimostriamo un risultato sulla cardinalità delle chiusure algebriche.

Proposizione 1.15. *Sia K un campo infinito. Allora $|\overline{K}| = |K|$.*

Dimostrazione. Considero $K \subset L_1$ con L_1 il campo costruito nella dimostrazione del teorema 1.13. Dico che $|K| = |L_1|$.
$L_1 = \bigcup_A K(\alpha)$ con $A = \{\alpha \text{ algebrico su } K\}$. Poiché ogni α algebrico é radice di un polinomio di $K[x]$, vale $|A| = |K[x]|$. Inoltre

$$|K| \leq |K[x]| \leq \sum_n |K[x]_{\leq n}| = \sum_n |K^{n+1}| = |K|$$

da cui $|K| = |K[x]|$. Allora

$$|K| \leq |L_1| \leq \sum_A |K(\alpha)| = |K||A| = |K||K[x]| = |K|$$

da cui $|K| = |L_1|$. Ma

$$|K| \leq |L| \leq \sum_i |L_i| = \aleph_0 |K| = |K|$$

da cui la tesi.

□

Da questo risultato si evince che $\mathbb{C}$ non é una chiusura algebrica di $\mathbb{Q}$, poiché $|\mathbb{Q}| = \aleph_0 < \mathfrak{c} = |\mathbb{C}|$.

1.2 Estensioni di omomorfismi

Siano K, L campi (non necessariamente un'estensione) e sia $\phi : K \to L$ un omomorfismo non nullo. Sia dunque F un sovracampo di K. Ci chiediamo se esiste un omomorfismo $\tilde{\phi}$: $F \to L$ che *estende* ϕ, ossia tale che $\tilde{\phi}|_K = \phi$. Siamo interessato in particolare al caso in cui F/K é un'estensione algebrica.

Analizziamo prima il caso delle estensioni algebriche semplici, ossia delle estensioni di K del tipo $F = K(\alpha)$ con α algebrico. Il problema è capire quali siano le possibili immagini di α; dato che α soddisfa un polinomio a coefficienti in K, esistono solo un numero finito di possibili immagini. Questo non sarebbe vero se α fosse trascendente su K. Sia $\mu(x)$ il polinomio minimo di α su K. Consideriamo l'omomorfismo di anelli indotto da ϕ

$$\varphi\colon K[x] \longrightarrow L[x]$$

tale che $\varphi(f) = \phi f$, dove $f(x) = \sum_{i=1}^n a_i x^i$ e $\phi f(x) = \sum_{i=1}^n \phi(a_i) x^i$.
Allora $\tilde{\phi}(\alpha)$ deve essere una delle radici di $\phi\mu(x)$ in L: poiché $\tilde{\phi}|_K = \phi$, posto $\mu(x) = \sum a_i x^i$, per linearità deve valere che

$$\phi\mu(\tilde{\phi}(\alpha)) = \sum_i \phi(a_i)(\tilde{\phi}(\alpha))^i = \tilde{\phi}(\sum_i a_i \alpha^i) = \tilde{\phi}(\mu(\alpha)) = \tilde{\phi}(0) = 0$$

Dunque condizione necessaria per estendere ϕ a $K(\alpha)$ é che $\phi\mu(x)$ abbia radici in L: in tal caso posso estenderlo in tanti modi quante sono tali radici in L. Da quanto visto, segue:

Proposizione 1.16. *Sia $F = K(\alpha)$ estensione algebrica di K, sia $\phi : K \hookrightarrow L$ omomorfismo iniettivo e sia $\mu(x)$ il polinomio di α su K. Se m é il numero di radici di $\phi\mu(x)$ in L, allora esistono esattamente m estensioni di ϕ a F. In particolare, se $L = \overline{K}$ e $i : K \hookrightarrow \overline{K}$, i ha tante estensioni quante sono le radici distinte di $\mu(x)$ in $\overline{K}$.*

Passiamo ora dal caso di estensioni semplici al caso di estensioni algebriche qualsiasi. Vale il seguente risultato:

Teorema 1.17. *Sia F/K un'estensione algebrica e sia Ω un'estensione algebricamente chiusa di K. Sia $\phi : K \hookrightarrow \Omega$ un omomorfismo iniettivo. Allora esiste $\tilde{\phi} : F \hookrightarrow \Omega$ tale che $\tilde{\phi}|_K = \phi$.*
In particolare, se Ω é anche algebrico su K e F é anche algebricamente chiuso, allora $\tilde{\phi}$ é un isomorfismo.

Dimostrazione. Consideriamo $\Gamma = \{(E, \tau) \mid K \subset E \subset F,\ \tau : E \hookrightarrow \Omega,\ \tau|_K = \phi\}$: allora $\Gamma \neq \emptyset$ poiché $(K, \phi) \in \Gamma$. Muniamo Γ di un ordinamento parziale

$$(E_1, \tau_1) \leq (E_2, \tau_2) \iff E_1 \subset E_2,\ \tau_2|_{E_1} = \tau_1$$

Vogliamo dunque vedere che Γ é un insieme induttivo. Sia $\mathcal{C} = \{(E_i, \tau_i)\}_i$ una catena in Γ: prendo $E = \bigcup_i E_i$ e $\tau : E \hookrightarrow \Omega$ tale che $\tau(\gamma) = \tau_n(\gamma)$ se $\gamma \in E_n$ (é ben definito per definizione dei τ_i). Allora (E, τ) é un maggiorante di $\mathcal{C}$. Per il lemma di Zorn, esiste $(E_0, \tau_0) \in \Gamma$ massimale rispetto l'ordinamento. Dico che $E_0 = F$: se fosse $E_0 \neq F$, allora esisterebbe $\alpha \in F - E_0$ e quindi potremmo considerare l'estensione semplice $E_0(\alpha)$ e un'estensione di τ_0 a $E_0(\alpha)$ (sia essa τ_0'), avendo dunque un nuovo elemento massimale che contiene strettamente (E_0, τ_0) (assurdo). Segue che τ_0 é l'estensione di ϕ a F cercata.

□

Corollario 1.18. *La chiusura algebrica di un campo é unica a meno di isomorfismi.*

Prima abbiamo visto che nel caso di estensioni semplici ci sono tante estensioni di ϕ: $K \hookrightarrow \overline{K}$ quante le radici di $\phi\mu$ (nelle stesse notazioni precedenti). Vediamo ora che il numero di estensioni é anche uguale al numero di radici di μ (e dunque che μ e $\phi\mu$ hanno lo stesso numero di radici).

Proposizione 1.19. *Sia $K(\alpha)$ un'estensione algebrica di K e sia μ il polinomio minimo di α su K di grado n. Sia ϕ: $K \hookrightarrow \overline{K}$. Se μ ha m radici distinte in $\overline{K}$, allora ϕ si estende a $K(\alpha)$ in m modi.*

Dimostrazione. Siano $\alpha_1, \ldots, \alpha_m$ le radici di μ: quindi in $\overline{K}[x]$

$$\mu(x) = (x - \alpha_1)^{e_1} ... (x - \alpha_m)^{e_m}$$

Estendiamo ϕ a $\tilde{\phi}$: $\overline{K} \to \overline{K}$, applicandolo a μ: si ha

$$\phi\mu(x) = (x - \tilde{\phi}(\alpha_1))^{e_1} ... (x - \tilde{\phi}(\alpha_m))^{e_m}$$

Le $\tilde{\phi}(\alpha_i)$ sono tutte distinte poiché gli omomorfismi non nulli di campi sono iniettivi, da cui la tesi. □

1.3 Campi di spezzamento ed estensioni normali

Definizione 1.20. Data $\mathfrak{F} = \{f_i\}_{i\in I} \subset K[x]$ una famiglia di polinomi di grado positivo, un sovracampo L di K si dice **campo di spezzamento** della famiglia $\mathfrak{F}$ su K se

- ogni f_i si spezza linearmente in $L[x]$;
- F/K é generata dalle radici degli f_i in L.

Notiamo che, fissata una chiusura algebrica $\overline{K}$, se $f \in K[x]$ si scrive come $f(x) = (x-\alpha_1)^{e_1}...(x-\alpha_n)^{e_n}$ in $\overline{K}[x]$, allora $L = K(\alpha_1, ..., \alpha_n)$ è l'*unico* campo di spezzamento di f su K per unicità della fattorizzazione in $\overline{K}[x]$.

D'ora in avanti per comodità useremo l'abbreviazione *cds* in luogo di *campo di spezzamento.*

Proposizione 1.21. *Data $\mathfrak{F} = \{f_i\}_{i\in I} \subset K[x]$ con $\deg f_i \geq 1$, siano L ed L_S i campi di spezzamento rispettivamente di $\mathfrak{F}$ e di $\{f_i\}_{i\in S}$ su K, al variare di S tra i sottoinsiemi finiti di I. Allora vale*

$$L = \bigcup_{S\subset I \text{ finito}} L_S = \prod_{S\subset I \text{ finito}} L_S$$

dove con $\prod$ indico il composto di campi.

Dimostrazione. La prima uguaglianza è vera per definizione. Vediamo la seconda. $\prod L_S$ é il composito di campi, e quindi é il piú piccolo sottocampo di $\overline{K}$ contenente tutti i L_S: dunque $\bigcup L_S \subset \prod L_S$. D'altra parte, $\bigcup L_S$ é un campo (poiché $\{S \subset I \text{ finito}\}$ é un insieme filtrante). Quindi vale l'uguaglianza.

□

In generale, due campi di spezzamento di un polinomio su un campo posso essere in due chiusure algebriche diverse. Col prossimo risultato mostriamo che il campo di spezzamento è unico a meno di isomorfismi.

Lemma 1.22. *Siano L, L' campi di spezzamento di $\mathfrak{F} = \{f_i\}_{i\in I}$ su K. Allora per ogni omomorfismo $\sigma\colon L \to \overline{L'}$ tale che $\sigma|_K = id$, vale $\sigma(L) = L'$.*

Dimostrazione. Per la proposizione precedente, basta mostrarlo per $\mathfrak{F} = \{f\}$. Sia $f = c(x-\alpha_1)^{e_1}...(x-\alpha_m)^{e_m}$. Poiché $f \in K[x]$, $f = \sigma f$. Ma in $\overline{L'}[x]$ si ha che $\sigma f = c\prod_{i=1}^{m}(x-\sigma(\alpha_i))^{e_i}$. Allora

$$L' = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)) = \sigma(K(\alpha_1, \ldots, \alpha_m)) = \sigma(L)$$

□

Corollario 1.23. *Siano $L, L' \subseteq \mathbb{K}$ due campi di spezzamento di $\mathfrak{F}$ su K. Allora $L = L'$.*

Definizione 1.24. Un'estensione algebrica F/K è **normale** se

$$\forall\ \phi : F \to \overline{F} \text{ tale che } \phi|_K = id,\ \ \sigma(F) = F$$

In realtà nella definizione è sufficiente richiedere che valga uno dei due contenimenti:

Proposizione 1.25. *Sia F/K un'estensione algebrica e sia $\phi : F \to \overline{F}$ tale che $\phi|_K = id$ e $\phi(F) \subset F$. Allora $\phi(F) = F$.*

Dimostrazione. È sufficiente mostrare la surgettività di ϕ; sia allora $\alpha \in F$. L'orbita di α tramite ϕ è contenuta nell'insieme delle radici di μ_α

$$\{\phi^i(\alpha)\} \subseteq \{\text{radici di } \mu_\alpha\}$$

Di conseguenza ϕ agisce come una permutazione dell'orbita (perché questa è finita e ϕ è iniettiva) e dunque esiste $\beta = \phi^j(\alpha)$ tale che $\phi(\beta) = \alpha$, da cui la tesi. □

Teorema 1.26. *Sia F/K un'estensione algebrica. Sono equivalenti:*

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

Dimostrazione.

(1) ⇒ (2) Sia $f \in K[x]$ irriducibile, sia $\mu \in K[x]$ il polinomio minimo delle radici di f ($f \sim \mu$). Sia $\alpha \in F$ radice di μ e consideriamo l'immersione $\sigma\colon K(\alpha) \to \overline{F}$ tale che $\sigma(\alpha) = \beta$, dove β è una radice di $\sigma\mu = \mu$ (perché $\sigma|_K = id$). σ si estende a $\phi : F \to \overline{F}$ e quindi $\phi(\alpha) = \beta$. Ma $\phi(F) = F$ per normalità di F su K, quindi $\beta \in F$. Ne segue che tutte le radici di μ sono in F e quindi $\mu \sim f$ si spezza in fattori lineari su F.

(2) ⇒ (3) Sia $\mathfrak{F} = \{\mu_\alpha \mid \alpha \in F,\ \mu_\alpha \text{ pol. min. di } \alpha \text{ su } K\}$. Chiaramente F è il campo di spezzamento di $\mathfrak{F}$: detto infatti E quest'ultimo, si ha che $E \supseteq F$. D'altronde ognuno dei μ_α si spezza completamente in F e dunque $E \subseteq F$, da cui la tesi.

(3) ⇒ (1) Segue dal lemma 1.22 con $F = L = L'$.

□

Esempio.

- $\mathbb{Q}(\sqrt{p} \mid p \text{ primo})$ è normale su $\mathbb{Q}$ in quanto è il campo di spezzamento di $\{x^2 - p\}_p$.

- $\mathbb{Q}(\zeta_m \mid m \geq 2)$ è normale su $\mathbb{Q}$ in quanto campo di spezzamento di $\{x^m - 1\}_m$.
- $\mathbb{F}_p(\sqrt{a} \mid a \in \mathbb{F}_p) = \mathbb{F}_{p^2}$ è normale su $\mathbb{F}_p$ poiché campo di spezzamento di $\{x^2 - a\}_a$.
- $\mathbb{F}_p(\zeta_m \mid m \geq 2) = \overline{\mathbb{F}}_p$ (dunque é normale) in quanto in $\overline{\mathbb{F}}_p$ ho tutti elementi di ordine finito.

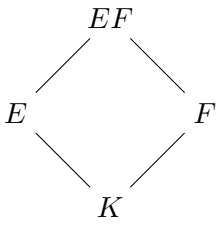
Studiamo ora le proprietà delle estensioni normali:

- **torri**: la proprietà delle torri non vale. Vediamo nel dettaglio:

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

  - L/K normale $\implies$ L/F normale.
  - L/K normale $\not\Rightarrow$ F/K normale: per esempio
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{2})$$
  - F/K, L/F normali $\not\Rightarrow$ L/K normale: per esempio
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

- **shift**: Vale la proprietà dello shift, ossia se E/K normale allora EF/F normale. Infatti, dato ψ omomorfismo, $\psi(EF) = \psi(E)\psi(F) = \psi(E)F$. Notiamo che $\psi|_E \colon E \to \overline{EF}$; dato che E è algebrico su K e $\psi|_K = id$, allora $\psi|_E \colon E \to \overline{E}$ da cui $\psi(E) = E$ per normalità.
- **composto**: Vale la proprietà del composto, ossia se E/K e F/K sono normali, allora lo è anche EF/K; infatti $\psi(EF) = \psi(E)\psi(F) = EF$



Notiamo che vale anche che l'intersezione di estensioni normali è normale. Infatti dato $\psi \colon E \cap F \to \overline{K}$ si ha che ψ si estende a

$$\psi_1 \colon E \to E \qquad\qquad \psi_2 \colon F \to F$$

Di conseguenza $\psi(E \cap F) = \psi_1(E) \cap \psi_2(F) = E \cap F$.

Nelle estensioni normali, la fattorizzazione di un polinomio irriducibile rispetta delle condizioni sui gradi:

Proposizione 1.27. *Sia L/K un'estensione normale, sia $f \in K[x]$ monico e irriducibile su K e sia $f = f_1...f_r$ la fattorizzazione in irriducibili in $L[x]$ (non necessariamente distinti). Allora per ogni i, j esiste un omomorfismo di campi*

$$\sigma \colon L \longrightarrow L,\ \sigma|_K = id$$

tale che $\sigma(f_i) = f_j$.

Dimostrazione. Sia α una radice di f_i e β una radice di f_j. Sappiamo che esiste un'immersione $\sigma \colon K(\alpha) \to \overline{K}$ tale che $\sigma(\alpha) = \beta$. Possiamo estendere σ a $\tilde{\sigma} \colon L \to L$ (per normalità di L) e dunque $\sigma(f_i) = f_j$, da cui la tesi. □

Segue direttamente dalla proposizione che ogni fattore debba avere lo stesso grado; questo è falso in generale.

Definizione 1.28. Sia F/K un'estensione algebrica e siano $\{\phi_i : F \to \overline{F}\}_{i \in I}$ le immersioni di F/K in $\overline{K}$. Definiamo la **chiusura normale** di F/K il campo

$$\tilde{F} = \prod_{i \in I} \phi_i(F)$$

Esempio. Dati $F = K(\alpha)$ e $\mu_\alpha = (x-\alpha_1)^{e_1}...(x-\alpha_n)^{e_n}$, la chiusura normale di F su K è

$$\tilde{F} = \prod K(\alpha_i)$$

Proposizione 1.29.

1. *$\tilde{F}$ è la minima estensione normale di K contenente F.*
2. *F/K finita $\implies$ $\tilde{F}/K$ finita.*

Dimostrazione.

1. $\tilde{F}/K$ è normale: data $\sigma \colon \tilde{F} \to \overline{K}$ tale che $\sigma|_K = id$, vale

   $$\sigma(\phi_i F) = \sigma\phi_i(F) = \phi_j(F) \subset \tilde{F}$$

   da cui $\sigma(\tilde{F}) \subset \tilde{F}$. Inoltre, $\tilde{F}$ è la minima estensione normale su K che contiene F. Infatti, sia L un'estensione normale che contiene F. Possiamo estendere ogni ϕ_i ad automorfismi di L (per normalità)

   $$\tilde{\phi}_i : L \to L,\ \tilde{\phi}_i|_F = \phi_i$$

   Allora $\phi_i(F) \subset \tilde{\phi}_i(L) = L$ per ogni i, da cui

   $$\tilde{F} = \prod \phi_i(F) \subset L$$

2. Dato che $[F : K] < \infty$, possiamo scegliere dei generatori di F su K $F = K(\alpha_1, \ldots, \alpha_n)$. Allora $\tilde{F}$ è il campo di spezzamento di $\{\mu_{\alpha_1}, \ldots, \mu_{\alpha_n}\}$, per cui $[\tilde{F} : K] < \infty$.

□

Oltre alla chiusura normale, che è la più piccola estensione normale su K di F, possiamo considerare la più grande sottoestensione di F normale su K. Questo è il nucleo normale:

Definizione 1.30. Sia $K \subset F$ un'estensione finita. Definisco il **nucleo normale** di F come

$$\underline{F} = \bigcap \phi_i(F)$$

Proposizione 1.31. *Il nucleo normale $\underline{F}$ di F/K è la massima sottoestensione di F normale su K.*

Dimostrazione. Mostriamo dapprima che $\underline{F}$ è normale. Sia $\phi\colon \underline{F} \to \overline{F}$; possiamo estendere ϕ a un'immersione $\tilde{\phi}$ di F in $\overline{F}$. Allora

$$\tilde{\phi}\Big(\cap \phi_i(F)\Big) \subseteq \cap \phi_i(F) = \underline{F}$$

da cui la normalità di $\underline{F}$.

Sia ora $L \subseteq F$ una sottoestensione di F normale su K. Notiamo che le immersioni di L coincidono con le restrizioni delle immersioni di F in $\overline{K}$. Dunque, per ogni immersione ϕ_i di F,

$$\phi_i(L) = L \subseteq \phi_i(F)$$

da cui $L \subseteq \cap \phi_i(F) = \underline{F}$. □

1.4 Separabilitá

Definizione 1.32. Sia $f \in K[x]$ un polinomio di grado positivo. f è **separabile** se le sue radici in $\overline{K}$ sono tutte distinte.

Notiamo che la definizione non dipende dalla chiusura algebrica $\overline{K}$: infatti se Ω è un'altra chiusura algebrica di K, allora esiste un isomorfismo $\sigma\colon \overline{K} \to \Omega$ con $\sigma|_K = id$. Se $f = \prod (x - \alpha_i)^{e_i}$ in $\overline{K}[x]$, allora $f = \sigma f = \prod (x - \sigma(\alpha_i))^{e_i}$ in $\Omega[x]$.

Lemma 1.33 (Criterio della derivata)**.** *Sia $f \in K[x]$ un polinomio di grado positivo. Allora:*

1. *f ha radici multiple se e solo se* $\gcd(f, f') \neq 1$*;*
2. *Supponiamo che f sia irriducibile. f ha radici multiple se e solo se $f' = 0$.*

Corollario 1.34. *Sia $f \in K[x]$ irriducibile. Allora:*

1. *(*$\operatorname{char} K = 0$*) f è separabile;*

2. *(*$\operatorname{char} K = p$*) posto* $r = \max\{k \in \mathbb{Z} \mid f(x) = g(x^{p^k})\}$,
   - *ogni radice di* f *ha molteplicità* p^r*;*
   - g *è irriducibile e separabile;*
   - *gli zeri di* f *sono le radici* p^r*-esime degli zeri di* g*.*

Dimostrazione.

1. Se f irriducibile, allora $f' \neq 0$ e dunque f è separabile.
2. g è irriducibile e separabile se e solo se $g' \neq 0$. Ma $g' = 0$ se e solo se $g(x) = h(x^p)$, il che è assurdo per la massimalità di r. Dunque g è irriducibile e separabile. Inoltre, $g = \prod_{i=1}^{n}(x-\alpha_i)$ in $\overline{K}[x]$ con $\alpha_i \neq \alpha_j$ per $i \neq j$. Dunque $f(x) = g(x^{p^r}) = \prod(x^{p^r} - \alpha_i)$. Sia $\beta_i \in \overline{K}$ tale che $\beta^{p^r} = \alpha_i$: allora $f(x) = \prod(x^{p^r} - \beta_i^{p^r}) = \prod(x - \beta_i)^{p^r}$, da cui la tesi.

□

Definizione 1.35. Sia $\alpha \in \overline{K}$. α è *separabile* su K se il suo polinomio minimo su K μ_α è separabile su K. Diciamo che l'estensione F/K è *separabile* se per ogni $\alpha \in F$, α è separabile su K.

Esempio. L'estensione

$$\mathbb{F}_p(t) \subset {}^{\mathbb{F}_p(t)[x]}\!\diagup_{(x^p - t)}$$

non è separabile. Infatti $f = x^p - t$ è irriducibile per Eisenstein e $f' = 0$.

Definizione 1.36. K è **perfetto** se ogni sua estensione algebrica è separabile.

Esempio.
- Ogni campo a caratteristica 0 è perfetto.
- I campi finiti $\mathbb{F}_{p^n}$ sono perfetti. Infatti se $f(x) = g(x^{p^r})$ con $r \geq 1$, allora
$$f(x) = \sum a_i x^{p^r i} = \sum a_i^p x^{p^r i} = \Big(\sum a_i x^i\Big)^{p^r}$$
- $\mathbb{F}_p(t)$ non è perfetto (basta vedere l'esempio precedente).

Definizione 1.37. Sia L/K un'estensione algebrica. Definiamo **grado di separabilità**

$$[L : K]_s = \#\operatorname{Hom}_K(L, \overline{K})$$

La definizione non dipende da $\overline{K}$, in quanto dato $\sigma\colon \overline{K} \to \Omega$ si ha la bigezione:

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

Osserviamo inoltre che, dato $\gamma : K \to \overline{K}$, vale

$$\#\operatorname{Hom}_K(L, \overline{K}) = \#\{\psi : L \to \overline{K} \mid \psi|_K = \gamma\}$$

Proposizione 1.38. *Sia $L = K(\alpha)$ con α algebrico su K e μ il suo polinomio minimo su K. Allora:*

1. $[L : K]_s = \#$*radici distinte di* μ *in* $\overline{K}$.
2. α *é separabile su* $K \iff [L : K]_s = [L : K]$.
3. *(*$\operatorname{char} K = p$*) se* p^r *é la molteplicitá di* α *in* μ, $[L : K] = p^r[L : K]_s$.

Dimostrazione.

1. Basta notare che $[L : K]_s = \#\operatorname{Hom}_K(K(\alpha), \overline{K}) = \#$ radici distinte di μ in $\overline{K}$.
2. Per definizione, α è separabile su K se e solo se μ ha tutte radici distinte. Dunque
$$[K(\alpha) : K]_s = \#\{\text{radici distinte di } \mu\} = \deg \mu = [K(\alpha) : K]$$
3. Sappiamo che μ ha tutte radici di molteplicità p^r e ha $[K(\alpha) : K]_s$ radici distinte, dunque $[K(\alpha) : K] = \deg \mu = p^r[K(\alpha) : K]_s$.

□

Lemma 1.39. *Sia $K \subset L \subset M$ una torre di estensioni algebriche. Allora*
$$[M : K]_s = [M : L]_s[L : K]_s$$

Dimostrazione. Considero $K \subset L \subset M \subset \overline{K}$. Allora
$$[M : L]_s = \#\operatorname{Hom}_L(M, \overline{K}) = \#\{\tau_j\}_{j\in J}$$
$$[L : K]_s = \#\operatorname{Hom}_K(L, \overline{K}) = \#\{\sigma_i\}_{i\in I}$$

Siano $\overline{\sigma}_i$ le estensioni dei σ_i a $\overline{K}$. Mostriamo che:

- $\overline{\sigma}_i \circ \tau_j$ sono tutti distinti al variare di i, j e $\{\overline{\sigma}_i \circ \tau_j\} \subseteq \operatorname{Hom}_L(M, \overline{K})$.
- Ogni $\gamma \in \operatorname{Hom}_K(M, \overline{K})$ si scrive come $\overline{\sigma}_i \circ \tau_j$.

Per mostrare il primo punto, basta notare che se
$$\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_l \circ \tau_k$$
allora la loro restrizione a L deve coincidere; dato che $\tau_j|_L = id$ si ha $i = l$. Da questo segue allora $j = k$ e quindi il primo punto.
Per il secondo punto, sia $\gamma|_L \in \operatorname{Hom}_K(L, \overline{K})$. Notiamo che esiste $\gamma|_L = \sigma_i$ per un certo $i \in I$. Di conseguenza, $\overline{\sigma}_i^{-1} \circ \gamma \in \operatorname{Hom}_L(M, \overline{K})$ e quindi $\overline{\sigma}_i^{-1} \circ \gamma = \tau_j$, da cui $\gamma = \overline{\sigma}_i \circ \tau_j$. □

La moltiplicatività del grado di separabilità permette di generalizzare i risultati visti sulle estensioni semplici alle estensioni finite:

Corollario 1.40. *Sia L/K un'estensione finita. Allora:*

1. *(*$\operatorname{char} K = 0$*)* $[L : K]_s = [L : K]$.
2. *(*$\operatorname{char} K = p$*)* $[L : K] = p^r[L : K]_s$.

Teorema 1.41 (Caratterizzazione estensioni separabili finite)**.** *Sia L/K un'estensione finita. Sono equivalenti:*

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

Dimostrazione.

(1) $\Rightarrow$ (2) Ovvio.

(2) $\Rightarrow$ (3) Per la formula dei gradi di estensioni finite e per il lemma 1.39, possiamo ricondurci al caso semplice e concludere per il punto (2) della proposizione 1.38.

(3) $\Rightarrow$ (1) Poiché i campi a caratteristica 0 sono perfetti, resta da analizzare solo il caso $\operatorname{char} K = p$. Sia $\alpha \in L$ e μ il suo polinomio minimo su K. Sappiamo da 1.38 che $[K(\alpha) : K] = p^r[K(\alpha) : K]_s$, per cui α è separabile se e solo se $r = 0$. Ma

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \qquad [L : K]_s = [L : K(\alpha)]_s[K(\alpha) : K]_s$$

e per ipotesi vale l'uguaglianza tra le due espressioni. Ne segue che $[K(\alpha) : K] = [K(\alpha) : K]_s$, ossia $r = 0$.

□

Corollario 1.42. *Sia $K \subset K(S) = L$ un'estensione algebrica. Sono equivalenti:*

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

Inoltre, se valgono (1) *e* (2)*, si ha anche*

3. $[L : K] = [L : K]_s$

Dimostrazione.

(1) $\Rightarrow$ (2) Ovvio.

(2) $\Rightarrow$ (1) Sia $\alpha \in L$; per definizione di $L = K(S)$, $\alpha \in K(\alpha_1, \ldots, \alpha_n) = F$ con $\{\alpha_i\} \subset S$. Per il teorema precedente, F/K è separabile e dunque α è separabile su K.

(1), (2) $\Rightarrow$ (3) Se l'estensione è finita, segue dal teorema precedente. Supponiamo allora che $[L : K] = \infty$. Allora per ogni $n \in \mathbb{N}$ esiste un sottocampo M_n tale che $n < [M_n : K] < \infty$. L'estensione M_n/K è separabile e quindi $[M_n : K]_s = [M_n : K] > n$ per ogni $n \in \mathbb{N}$. Ne segue che $[L : K]_s = \infty$.

□

Notiamo che il terzo punto del corollario non è in generale sufficiente per garantire la separabilità dell'estensione. Consideriamo per esempio l'estensione

$$K = \mathbb{F}_p(t) \subset \overline{\mathbb{F}_p(t)} = L$$

Allora L/K non è separabile in quanto tra le sottoestensioni vi è anche

$$F = {}^{K[x]}\!/_{(x^p - t)}$$

che non è separabile. D'altronde il grado di separabilità è infinito; infatti tra le sottoestensioni vi è anche $E = \overline{\mathbb{F}_p}(t)$ che è separabile (perché separabilmente generata) e infinita. Di conseguenza il grado di separabilità coincide con il grado dell'estensione ma questa non è separabile.

Vediamo ora le proprietà delle estensioni separabili:

- **torri**: Vale che

$${}^{L}\!/_{K} \text{ è separabile } \iff {}^{L}\!/_{F},\ {}^{F}\!/_{K} \text{ sono separabili}$$

Se L/K è finita, segue dalla moltiplicatività del grado (1.39). Vediamo il caso in cui L/K non è finita:

$\Rightarrow$ Sia $\alpha \in L$ e μ il suo polinomio minimo su K: allora μ ha radici tutte distinte (poiché α è separabile su K). Ma allora μ è polinomio minimo a radici distinte anche in F, dunque L/F é separabile. D'altra parte, preso $\beta \in F \subset L$, sia μ' il suo polinomio minimo su K: poiché $\beta \in L$, μ' ha radici distinte. Dunque anche F/K è separabile.

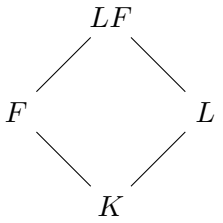
$\Leftarrow$ Sia $\alpha \in L$ e $\mu_F \in F[x]$ il suo polinomio minimo su F

$$\mu_F = x^n + \sum_{i=0}^{n-1} a_i x^i$$

che ha radici distinte per ipotesi. Consideriamo allora $F_0 = K(a_0, \ldots, a_{n-1})$ e le estensioni $K \subset F_0 \subset F_0(\alpha)$: poiché sono estensioni finite e separabili, α è separabile su K.

- **shift**:Vale che

$$F/K \text{ è separabile} \implies LF/L \text{ è separabile}$$



  Consideriamo infatti $\alpha \in F$ separabile su K. Allora α è separabile su L; dunque LF/L è generata da elementi separabili.

- **composto**: Vale che

$$F/K,\ L/K \text{ sono separabili} \implies LF/K \text{ è separabile}$$

  Questo segue dal fatto che la proprietà delle torri e dello shift implicano la proprietà del composto.

Dalla proprietà del composto segue anche che se L/K è separabile e $\tilde{F}$ è la chiusura normale di L su K, allora $\tilde{F}/K$ è separabile, in quanto composto dei coniugati di L, che sono separabili.

Nel caso di un'estensione finita e separabile vale il teorema dell'elemento primitivo:

Teorema 1.43 (Teorema dell'elemento primitivo)**.** *Sia $K \subset F$ un'estensione finita e separabile. Allora F è un'estensione semplice di K, ossia esiste $\gamma \in F$ tale che $F = K(\gamma)$.*

Dimostrazione. Supponiamo dapprima che F sia un campo finito. In questo caso, F è semplice: infatti $F^\times$ è sottogruppo moltiplicativo finito di un campo, dunque è ciclico. Se $F^\times =< \zeta >$, allora $F = K(\zeta)$.
Sia dunque K campo infinito. Poiché l'estensione è finita, possiamo scegliere un numero finito di generatori di $F = K(\alpha_1, \ldots, \alpha_n)$. Analizziamo il caso $n = 2$ (la tesi seguirà per induzione) e sia quindi $F = K(\alpha, \beta)$. Poiché F è separabile su K,

$$[F : K] = n = \#\operatorname{Hom}_K(F, \overline{K}) = [F : K]_s$$

Sia $\operatorname{Hom}_K(F) = \{\sigma_1, \ldots, \sigma_n\}$: mostriamo che esiste $\gamma \in F$ tale che γ ha n coniugati distinti ($\deg \mu_\gamma = n$). Ciò equivale a dire che $[K(\gamma) : K] = n$. Consideriamo gli elementi $\alpha + X\beta$ e il polinomio

$$f(X) = \prod_{i<j} (\sigma_i(\alpha) + X\sigma_i(\beta) - \sigma_j(\alpha) - X\sigma_j(\beta))$$

Notiamo che $f \neq 0$; se infatti

$$\sigma_i(\alpha) + X\sigma_i(\beta) = \sigma_j(\alpha) + X\sigma_j(\beta)$$

allora $\sigma_i(\alpha) = \sigma_j(\alpha)$ e $\sigma_i(\beta) = \sigma_j(\beta)$. Da questo seguirebbe $\sigma_i = \sigma_j$ (perché α e β generano F). Dato che $f \neq 0$ e K è infinito, esiste $t \in K$ tale che $f(t) \neq 0$, ossia $\sigma_i(\alpha) + t\sigma_i(\beta) \neq \sigma_j(\alpha) + t\sigma_j(\beta)$ per ogni $i \neq j$. Allora $\gamma = \alpha + t\beta$ ha n coniugati distinti, quindi $[K(\gamma) : K] = n$. □

Il teorema vale in realtà sotto condizioni molto più generali. In particolare, vale la seguente caratterizzazione:

Teorema 1.44. *Sia L/K un'estensione finita. Allora*

$$L/K \text{ è semplice} \iff \#\{F \mid K \subset F \subset L\} < \infty$$

Dimostrazione. Se K è finito, entrambe le condizioni sono sempre verificate. Supponiamo dunque che K sia un campo infinito.

($\Rightarrow$) Sia $L = K(\alpha)$ e sia μ il suo polinomio minimo. Consideriamo l'applicazione

$$\begin{array}{rccc} \psi\colon & \{F \text{ intermedi}\} & \longrightarrow & \{\text{divisori di } \mu\} \\ & F & \longmapsto & \mu_F \end{array}$$

dove abbiamo indicato con μ_F il polinomio minimo di α su F. Dato che il numero di divisori di μ sono in numero finito, è sufficiente mostrare l'iniettività della mappa. Osserviamo che $\mu_F | \mu_K$ per ogni F e che $\mu_F \in F_0[x]$, dove F_0 è il sottocampo di L generato dai coefficienti del polinomio μ_F. Notiamo che $F_0 \subseteq F$ e dato che $\mu_F \in F_0[x]$, allora $\mu_F = \mu_{F_0}$. Di conseguenza

$$[L : F] = \deg \mu_F = \deg \mu_{F_0} = [L : F_0]$$

e dato che vale un contenimento, $F = F_0$. Da questo otteniamo l'iniettività della mappa perché

$$\mu_F = \mu_{F'} \implies \mu_F = \mu_{F_0} = \mu_{F'} \implies F = F_0 = F'$$

($\Leftarrow$) Supponiamo che $L = K(\alpha, \beta, \alpha_1, \ldots, \alpha_n)$ e mostriamo un metodo iterativo per ridurre il numero di generatori. Consideriamo la famiglia di elementi $\Gamma = \{\alpha + t\beta \mid t \in K\}$; poiché K è infinito, $\#\Gamma = \infty$. Consideriamo le sottoestensioni $K \subset K(\alpha + t\beta) \subset L$: visto che le estensioni intermedie sono in numero finito e K è infinito, esistono $t_1, t_2 \in K$ tali che $K(\alpha + t_1\beta) = K(\alpha + t_2\beta)$. Allora $(t_1 - t_2)\beta \in K(\alpha + t_1\beta)$ e dunque $\beta \in K(\alpha + t_1\beta)$. Di conseguenza $\alpha, \beta \in K(\alpha + t_i\beta)$ e abbiamo ridotto il numero di generatori di $L = K(\alpha + t_1\beta, \alpha_1, \ldots, \alpha_n)$. Induttivamente, si ottiene che L è semplice.

□

Mostriamo ora un'esempio di estensione non semplice:

Esempio. Sia $K = \mathbb{F}_p(X^p, Y^p)$ e sia $L = \mathbb{F}_p(X, Y)$. Consideriamo l'automorfismo di Frobenius

$$\begin{array}{rccc} \phi\colon & L & \longrightarrow & L \\ & \alpha & \longmapsto & \alpha^p \end{array}$$

Si verifica facilmente che $K = \phi(L)$. Mostriamo che L/K ha grado p^2. Chiaramente $L = K(X, Y)$. Inoltre, $K(X) \cong \dfrac{K[t]}{(t^p - X^p)}$, con $t^p - X^p \in K[t]$ irriducibile poiché

$$[K(X) : K]_s = 1,\ [K(X) : K] \neq 1 \implies [K(X) : K] = p$$

Allo stesso modo, si mostra che $[L : K(X)] = [K(X)(Y) : K(X)] = p$ da cui $[L : K] = p^2$. Mostriamo ora che l'estensione non è semplice. Sia $\alpha \in L$; allora, dato che K è immagine del Frobenius, $\alpha^p \in K$ e dunque $\mu_\alpha \mid t^p - \alpha^p \in K[t]$. Ne segue che $\deg \mu_\alpha \leq p$ e dunque non può esistere un elemento primitivo. In base al teorema precedente, possiamo quindi trovare infiniti sottocampi; per esempio, le estensioni

$$L_i = K(X + tY) \qquad\qquad t \in K$$

sono tutte distinte (se due coincidessero, avremmo trovato un elemento primitivo).

1.5 Estensioni puramente inseparabili

Sia K campo e sia $\alpha \in \overline{K}$. Dalla proposizione 1.38 sappiamo che $\mu_\alpha(x) = g(x^{p^r})$ (con r massimo), da cui

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

Quindi $K(\alpha^{p^r})$ è la massima sottoestensione separabile di $K(\alpha)/K$.

Definizione 1.45. Data $K \subset L$ finita, definiamo **grado di inseparabilità** di L su K

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

Notiamo che:

- L/K finita e separabile $\iff [L:K]_i = 1$;
- se L/K è finita, allora $[L:K]_i = p^r$ (dove $p = \operatorname{char} K$).

Dalla moltiplicatività del grado di separabilità discende anche quella del grado di inseparabilità:

Proposizione 1.46. *Data $K \subset F \subset L$ torre di estensioni finite, vale*

$$[L:K]_i = [L:F]_i[F:K]_i$$

Definizione 1.47. $f \in K[x]$ è detto **puramente inseparabile** se ammette un'unica radice in $\overline{K}$. $\alpha \in \overline{K}$ è detto **puramente inseparabile** su K se μ_α è puramente inseparabile. L/K è detta **puramente inseparabile** se ogni $\alpha \in L$ è puramente inseparabile su K.

Si noti che:

- Se $\operatorname{char} K = 0$, allora f è puramente inseparabile se e solo se $f = (x-c)^m$.
- Se $\operatorname{char} K = p$, allora f è puramente inseparabile se e solo se $f = x^{p^r} - c$.

Dalla definizione discende anche che ogni estensione L/K puramente inseparabile è normale: infatti per ogni $\alpha \in L$, μ_α ha α come unica radice, dunque L è il campo di spezzamento di μ_α. Notiamo anche che se un'estensione L/K è sia separabile che puramente inseparabile, allora è banale. Sia infatti $\alpha \in L$ puramente inseparabile su K. Allora μ_α puramente inseparabile e dunque ammette un'unica radice in $\overline{K}$. D'altronde μ_α è anche separabile e dunque μ_α ha tutte le radici distinte. Dunque $\mu_\alpha(x) = x - \alpha$ e quindi $\alpha \in K$.

Proposizione 1.48. *Sia L/K algebrica di caratteristica p. Sono equivalenti:*

1. *L/K è puramente inseparabile;*
2. *esiste un sottoinsieme $S \subset L$ tale che $L = K(S)$ e per ogni $\gamma \in S$, γ è puramente inseparabile su K;*
3. *$[L:K]_s = 1$;*
4. *Per ogni $\alpha \in L$, esiste $r \geq 0$ tale che $\alpha^{p^r} \in K$.*

Inoltre, se L/K è finita, sono tutti equivalenti a $[L:K] = [L:K]_i$.

Dimostrazione.

(1) $\Rightarrow$ (2) Basta considerare $L = K(L)$.

(2) $\Rightarrow$ (3) Sia $\sigma \in \mathrm{Hom}_K(L)$ e $\gamma \in S$. Allora $\sigma(\gamma) = \gamma$, in quanto l'unica radice del polinomio minimo di γ è γ stesso. Ma allora $\sigma = id$, in quanto è l'identità sui generatori.

(3) $\Rightarrow$ (4) Dato $\alpha \in L$, $[K(\alpha) : K]_s = 1$, quindi μ_α è puramente inseparabile su K, cioé $\mu_\alpha(x) = x^{p^r} - \alpha^{p^r} \in K[x]$.

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

□

Vediamo ora le *proprietá delle estensioni puramente inseparabili*:

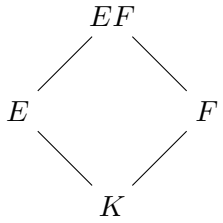
- **torri**:

  ${}^{L}\!/_{K}$ è puramente inseparabile $\iff$ ${}^{L}\!/_{F}$, ${}^{F}\!/_{K}$ sono puramente inseparabili

  Segue dalla moltiplicatività del grado di seprabilità.

- **shift**:

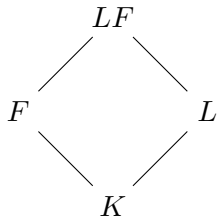
  ${}^{E}\!/_{K}$ è puramente inseparabile $\implies$ ${}^{EF}\!/_{F}$ è puramente inseparabile



  Infatti $EF = F(E)$ è generata da elementi puramenti inseparabili su K, dunque su F.

- **composto**:

  ${}^{E}\!/_{K}$, ${}^{F}\!/_{K}$ è puramente inseparabile $\implies$ ${}^{EF}\!/_{K}$ è puramente inseparabile



  Segue da *torri + shift*.

Definizione 1.49. Definiamo la **chiusura separabile** di K in $\overline{K}$ il campo prodotto delle estensioni separabili intermedie

$$K_s := \prod_{K \subset F \subset \overline{K} \text{ sep.}} F$$

ossia la massima estensione separabile di K contenuta in $\overline{K}$.

Teorema 1.50. *Sia L/K un'estensione algebrica e sia K_s la chiusura separabile di L su K. Allora K_s è univocamente determinato dalle proprietà*

$$\begin{array}{c} L \\ \Big| \ \textit{pur. insep.} \\ K_s \\ \Big| \ \textit{sep.} \\ K \end{array}$$

Inoltre, $[K_s : K] = [L : K]_s$ e, se definito, $[L : K_s] = [L : K]_i$.
Inoltre, se L/K è normale allora K_s/K è normale.

Dimostrazione. Mostriamo che L/K_s è puramente inseparabile. Dato $\alpha \in L$, sappiamo che esiste $r \in \mathbb{N}$ tale che $\mu(x) = g(x^{p^r})$ con g separabile e irriducibile. Consideriamo il diagramma

$$\begin{array}{ccccc} & & K_s(\alpha) & & \\ & \swarrow & & \searrow & \\ K(\alpha) & & & & K_s \\ & \searrow & & \swarrow & \\ \text{pur. insep.} & & K(\alpha^{p^r}) & & \\ & & \Big| \ \text{sep.} & & \\ & & K & & \end{array}$$

Dato che $K(\alpha)/K(\alpha^{p^r})$ è puramente inseparabile, per lo shift lo è anche $K_s(\alpha)/K_s$. Allora α è puram. insep. su K_s.
Vediamo che K_s è l'unico con tali proprietà. Sia $K \subset F \subset L$ tale che F/K è separabile e L/F è puram. insep. Consideriamo il diagramma

$$\begin{array}{ccccc} & & L & & \\ & \swarrow & & \searrow & \\ \text{pur. insep.} & & & & \text{pur. insep.} \\ & \searrow & & \swarrow & \\ F & & & & K_s \\ & \searrow & & \swarrow & \\ \text{sep.} & & & & \text{sep.} \\ & & K & & \end{array}$$

Dato che F/K è separabile, $F \subset K_s$ e quindi K_s/F è separabile da cui $F = K_s$. Inoltre:

- $[K_s : K] = [L : K]_s$ poiché $[L : K]_s = [L : K_s]_s[K_s : K]_s = [K_s : K]$;
- $[L : K_s] = [L : K]_i$ poiché $[L : K]_i = [L : K_s]_i[K_s : K]_i = [L : K_s]$;
- se L/K è normale e $\alpha \in K_s$, μ_α si spezza completamente su L per normalità e ogni radice di μ_α è separabile su K (poiché lo è α). Quindi le radici di μ_α sono separabili e sono in K_s. Ne segue che K_s/K è normale.

□

Vediamo ora che nel caso di un'estensione *normale* possiamo spezzare l'estensione nel modo inverso:

Teorema 1.51. *Sia L/K un'estensione normale. Allora esiste un'unica sottoestensione K_i tale che*

$$\begin{array}{c} L \\ \Big| \ sep. \\ K_i \\ \Big| \ pur.\ insep. \\ K \end{array}$$

Dimostrazione. Per normalità, $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$. Poniamo $K_i = L^{\mathrm{Aut}_K(L)} = \mathrm{Fix}(\mathrm{Aut}_K(L))$: questo è un campo contenente K. Mostriamo che soddisfa le proprietà richieste.

- K_i/K è puramente inseparabile; se $\phi : K_i \to \overline{K}$ è un'immersione di K_i su K, possiamo estenderla a $\tilde{\phi} \in \mathrm{Aut}_K(L)$ e per definizione di K_i ho $id = \tilde{\phi}|_{K_i} = \phi|_{K_i} = \phi$, cioè $[K_i : K]_s = 1$.
- K_i è la massima sottoestensione di L/K puramente inseparabile: infatti ogni estensione di questo tipo è fissata da $\mathrm{Aut}_K(L)$.
- L/K_i è separabile: dato $\alpha \in L$, consideriamo l'orbita di α

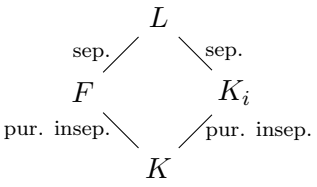
  $$\mathrm{orb}_{\mathrm{Aut}_K(L)}(\alpha) = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$$

  Allora il polinomio

  $$f(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$$

  è a coefficienti in K_i in quanto $\mathrm{Aut}_K(L)$ permuta soltanto i σ_i. Dunque α è separabile su K_i in quanto radice di f che è separabile.

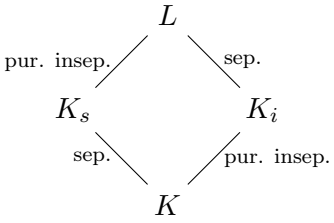
- K_i è unico: sia $K \subset F \subset L$ tale che F/K è puramente inseparabile e L/F è separabile. Abbiamo il diagramma



  Ma F/K è puramente inseparabile e dunque K_iF viene fissato da ogni automorfismo. Di conseguenza $F \subset K_i$, quindi K_i/F è puramente inseparabile; ma L/F è separabile e dunque K_i/F separabile. Ma ogni estensione separabile e puramente inseparabile è banale.

□

Abbiamo visto che l'ipotesi di *normalità* è sufficiente. In realtà è anche necessaria; infatti in una estensione non separabile non è detto che vi sia un elemento puramente inseparabile. Consideriamo il seguente diagramma



Notiamo che $K_i, K_s \subset K_iK_s \subset L$ ed essendo L/K_i separabile e L/K_s puram. insep., abbiamo che $K_iK_s = L$. Inoltre, K_i/K puram. insep. $\implies$ K_i/K normale.
Ora, se K_s/K fosse normale, lo sarebbe anche L/K (poiché composto di estensioni normali). Ma io cerco un'estensione L/K NON normale con tutte le sottoestensioni normali: ad esempio, posso cercare un'estensione L/K non normale con $[L : K] = 4$ e $[L : K]_s = [L : K]_i = 2$.

Esempio. $K = \mathbb{F}_2(X, Y)$, $L = K(\alpha)$ con α radice di $\mu_\alpha(t) = t^4 + Xt^2 + Y = g(t^2)$: il polinomio é irriducibile perché di Eisenstein rispetto al primo $\mathfrak{p} = (X, Y)$; inoltre, $[L : K]_s = [L : K]_i = 2$, in quanto $[L : K] = 4$ e $\mu_\alpha(t) = g(t^2)$ (dunque $[L : K]_i = 2$). Dunque mi basta vedere che L/K non é normale.
$g(z) = z^2 + xz + y = (z - \gamma)(z - \delta)$ in $\overline{K}$, quindi se $\gamma = \alpha^2$ e $\delta = \beta^2$, in $\overline{K}$ ho $\mu_\alpha(t) = (t - \alpha)^2(t - \beta)^2$.
Ma L/K normale $\iff$ $\beta \in L$. Se per assurdo $\beta \in L$, allora $\sqrt{X} = \alpha + \beta$, $\sqrt{Y} = \alpha\beta \in L$ e quindi $K(\sqrt{X}, \sqrt{Y}) \subset L$; 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). Dunque L/K non é normale.

1.6 Esercizi

Lemma 1.52. *Sia L/K un'estensione di campi con* $\operatorname{char} K = p$. *Sia $\alpha \in L$ algebrico su K. Dimostrare che*

$$\alpha \text{ è separabile su } K \iff K(\alpha) = K(\alpha^p)$$

Dimostrazione.

$\Rightarrow$ Sia μ_α il polinomio minimo di α su $K(\alpha^p)$: questo è separabile poiché $K(\alpha^p) \subset K(\alpha)$ é separabile. Ma $\mu_\alpha \mid X^p - \alpha^p$ che ha una sola radice, dunque $\mu_\alpha = X - \alpha$ da cui $\alpha \in K(\alpha^p)$.

$\Leftarrow$ Supponiamo per assurdo che α non sia separabile. Allora il polinomio minimo di α su K è del tipo $\mu_\alpha(x) = g(x^{p^r})$ con $r > 0$. Ne segue che $\mu_{\alpha^p} = g(x^{p^{r-1}})$, da cui

$$[K(\alpha^p) : K] = \deg \mu_{\alpha^p} = p^{r-1} \deg g$$
$$[K(\alpha) : K] = \deg \mu_\alpha = p^r \deg g$$

Poiché i due gradi sono diversi, $K(\alpha^p) \subsetneq K(\alpha)$ da cui un assurdo.

□

Proposizione 1.53. *Sia L/K un'estensione di campi e supponiamo che $L = K(\alpha, \beta)$ con α separabile e β puramente inseparabile. Allora $L = K(\alpha\beta) = K(\alpha + \beta)$.*

Dimostrazione. Dato che α è separabile, per il lemma precedente $K(\alpha) = K(\alpha^{p^r})$ per ogni $r \in \mathbb{N}$. Dato che β è puramente inseparabile, esiste $k \in \mathbb{N}$ tale che $\beta^{p^k} \in K$. Di conseguenza,

$$(\alpha\beta)^{p^k} \in K(\alpha\beta) \Rightarrow \alpha^{p^k} \in K(\alpha\beta) \Rightarrow K(\alpha) = K(\alpha^{p^k}) \subseteq K(\alpha\beta)$$

Di conseguenza, $\alpha \in K(\alpha\beta)$ e dunque $K(\alpha, \beta) \subseteq K(\alpha\beta)$. Lo stesso ragionamento si può seguire nel caso della somma, da cui la tesi. □

Bosch, pagina 114. Esercizi: dal 4 all'11.

Capitolo 2

Teoria di Galois

2.1 Estensioni di Galois

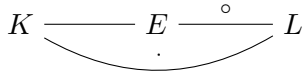
Definizione 2.1. Un'estensione algebrica L/K si dice **estensione di Galois** se è normale e separabile. Se L/K è di Galois, definiamo **gruppo di Galois** il gruppo

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$$

Si noti che, se L/K è di Galois, $|\mathrm{Gal}(L/K)| = [L : K]$. Vediamo le proprietà delle estensioni di Galois:

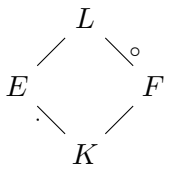
- **torri**:

$$L/K \text{ di Galois} \implies L/E \text{ di Galois} \quad (\text{ma } \not\Rightarrow E/K \text{ di Galois})$$



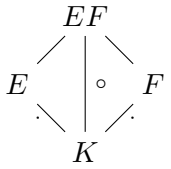
- **shift**:

$$E/K \text{ di Galois} \implies L/F \text{ di Galois}$$



- **composto**:

$$E/K,\ F/K \text{ di Galois} \implies EF/K \text{ di Galois}$$



Proposizione 2.2. *Sia L/K di Galois e sia $K \subset E \subset L$. Allora:*

1. $\mathrm{Aut}_E(L) < \mathrm{Aut}_K(L)$;
2. *E/K normale* $\implies \mathrm{Aut}_K(L) \xrightarrow{\cdot|_E} \mathrm{Aut}_K(E)$ *é surgettivo.*

Dimostrazione.

1. Segue banalmente da $K \subset E,\ \sigma|_E = id \implies \sigma|_K = id$.
2. Poiché E/K è normale, è ben definito $\mathrm{Aut}_K(E)$. La tesi segue dal teorema 1.17 e dalla normalità di L/K.

□

Vediamo ora un risultato, dovuto a Emil Artin, che ci permetterá di dimostrare il *teorema fondamentale della teoria di Galois.*

Lemma 2.3 (Lemma di Artin)**.** *Sia L un campo e sia G un sottogruppo di* $\mathrm{Aut}(L)$. *Sia $K = L^G = \mathrm{Fix}_L(G)$. Allora:*

1. *Se G è finito, allora L/K è di Galois finita e $G = \mathrm{Gal}(L/K)$.*
2. *Se G é infinito ed L/K è algebrica, allora L/K è di Galois infinita e $G < \mathrm{Gal}(L/K)$.*

Dimostrazione. Supponiamo dapprima che G sia finito, di cardinalità n. Mostriamo che L/K è di Galois. Dato $\alpha \in L$, si ha che $orb(\alpha) = \{\alpha_1, \ldots, \alpha_k\}$, con $k \leq n$. Di conseguenza il polinomio

$$p_\alpha(t) = \prod_{i=1}^{k}(x - \alpha_i)$$

è un polinomio che si annulla in α ed è a coefficienti in L^G, in quanto ogni elemento di G permuta gli α_i, lasciando invariato il polinomio. Questo mostra che L/L^G è algebrica è separabile, in quanto p è un polinomio separabile in $K[x]$ che si annulla in α. Inoltre, l'estensione è anche normale, in quanto campo di spezzamento dei p_α al variare di α in L. Inoltre, il ragionamento seguito mostra anche che ogni elemento ha al più n coniugati. Di conseguenza, ogni sottoestensione finita di L/K ha al più grado n per il teorema

dell'elemento primitivo. Da questo segue che L/K è finita e ha al più grado n. D'altronde,

$$n \geq [L:K] = [L:K]_s \geq n$$

dove l'ultima disuguaglianza è dovuta al fatto che $G \subseteq \mathrm{Hom}_K(L, \overline{K})$. Dunque $\mathrm{Gal}(L/K) = G$. Nel caso in cui G è infinito, è sufficiente notare che l'algebricità dell'estensione (che stavolta si ha per ipotesi) garantisce che l'orbita di ogni elemento sia finita. la dimostrazione di separabilità e normalità dell'estensione è dunque analoga al caso precedente. L'immersione del gruppo di Galois segue invece dalla definizione. □

Corollario 2.4. *Siano L/K normale e $G = \mathrm{Aut}_K(L)$. Allora L/L^G é di Galois e $G = \mathrm{Gal}(L/L^G)$. Inoltre, $L^G = K_i$ e, se L/K é separabile, $K = L^G$.*

Dimostrazione. Per 1.51 (si veda la dimostrazione), $L^G = K_i$, dunque L/L^G é normale (poiché lo é L/K) e separabile, ossia di Galois. Inoltre, per il Lemma di Artin (2.3), $\mathrm{Aut}_K(L) = G < \mathrm{Gal}(L/L^G) = \mathrm{Aut}_{L^G}(L) < \mathrm{Aut}_K(L)$, da cui $G = \mathrm{Gal}(L/L^G)$. □

Vediamo ora il *Teorema fondamentale della teoria di Galois*. Tuttavia, per ora enunciamo (e dimostriamo) solo una prima parte del Teorema, quella per gruppi di Galois *finiti*. Per la seconda parte (il caso infinito) dobbiamo aspettare di munire il gruppo di Galois di una topologia, detta *di Krull*.

Teorema 2.5 (Corrispondenza di Galois - parte I)**.** *Sia L/K di Galois e sia $G = \mathrm{Gal}(L/K)$. Allora esistono due mappe*

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

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

tali che $\phi \circ \psi = id$, ossia tali che ψ é iniettiva e ϕ é surgettiva.
Inoltre, F/K é 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 G é finito, vale anche $\psi \circ \phi = id$ (ossia ψ e ϕ sono bigettive) e

$$H \triangleleft G \iff L^H/K \text{ é di Galois}$$

Dimostrazione. Notiamo che ϕ e ψ sono ben definite (in particolare L/K di Galois $\implies$ L/F di Galois) e per il corollario precedente

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

Inoltre, F/K é di Galois $\iff \sigma(F) = F \ \forall\ \sigma : F \to \overline{K},\ \sigma|_K = id \iff \sigma(F) = F \ \forall\ \sigma \in \mathrm{Gal}(L/K)$; d'altra parte, $\mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K) \iff \sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/F)\ \forall\ \sigma \in \mathrm{Gal}(L/K)$.
Ma $\sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/\sigma(F))$ e $\sigma(F) = F\ \forall\ \sigma \in \mathrm{Gal}(L/K) \iff \mathrm{Gal}(L/\sigma(F)) = \mathrm{Gal}(L/F)$ (poiché ψ é iniettiva). Segue che F/K di Galois $\iff \mathrm{Gal}(L/F) \triangleleft \mathrm{Gal}(L/K)$ e, sapendo che $\cdot|_F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ é surgettiva, per il primo teorema di omomorfismo si ha

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

Supponiamo ora G *finito*. Dal lemma di Artin,

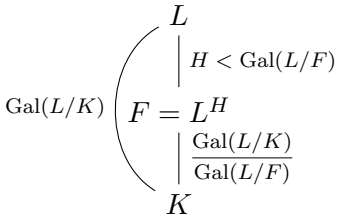
$$\psi \circ \phi(H) = \psi(L^H) = \mathrm{Gal}(L/L^H) \overset{2.3(1)}{=} H$$

dunque $\psi \circ \phi = id$ e (per quanto visto sopra)

$$H \overset{Artin}{=} \mathrm{Gal}(L/L^H) \triangleleft G \iff L/L^H \text{ di Galois}$$

□

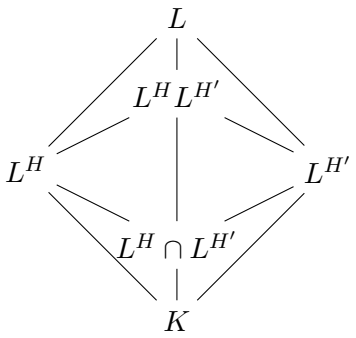
Vediamo che per estensioni *infinite*, in generale, è falso che ϕ sia iniettiva (dunque ψ surgettiva).
Controesempio: Considero $\overline{\mathbb{F}_p}/\mathbb{F}_p$ e $G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ il *gruppo assoluto di Galois* di $\mathbb{F}_p$. Sicuramente $\overline{\mathbb{F}_p}^G = \mathbb{F}_p$.
Sia ϕ il Frobenius di $\overline{\mathbb{F}_p}$; allora, posto $H = \langle\phi\rangle < G$, si ha $\overline{\mathbb{F}_p}^H = \mathbb{F}_p$. Dunque, se mostriamo che $H \lneq G$, abbiamo che esistono due sottogruppi di G che fissano lo stesso campo.
Ma $H \cong \mathbb{Z}$, quindi tutti i suoi sottogruppi hanno indice finito. Se si avesse $H = G$, si avrebbe che ogni sottocampo proprio F avrebbe grado $[F : \mathbb{F}_p]$ finito: ma ció é falso perché se $F = \bigcup_n \mathbb{F}_{p^{2^n}}$ si ha $[\overline{\mathbb{F}_p} : F] = [F : \mathbb{F}_p] = \infty$.
In generale, vale



Corollario 2.6. *Sia L/K finita e separabile. Allora L/K ha un numero finito di estensioni intermedie, dunque è semplice.*

Dimostrazione. La chiusura normale $\tilde{L}/K$ è di Galois finita, quindi $\mathrm{Gal}(\tilde{L}/K)$ è finito. Ne segue che le estensioni intermedie sono finite, in quanto corrispondono ai sottogruppi di un gruppo finito. □

Corollario 2.7. *Siano L/K di Galois finita, $G = \mathrm{Gal}(L/K)$ e il diagramma*



Allora:

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

Dimostrazione.

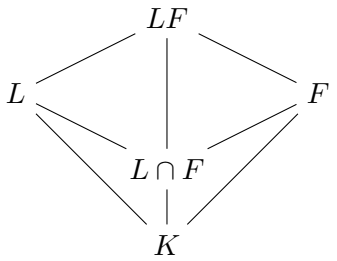
1. Segue dalla corrispondenza di Galois (2.5).
2. $L^H L^{H'} \subset L^{H \cap H'}$ é ovvia; l'altra inclusione segue da $\mathrm{Gal}(L/L^H L^{H'}) \subset \mathrm{Gal}(L/L^H) \cap \mathrm{Gal}(L/L^{H'})$ passando ai campi fissati.
3. Analogo al punto 2..

□

Il teorema che segue lo enunciamo nella sua forma generale, ma lo dimostriamo solo nel caso finito. Il caso infinito lo rinviamo a quando avremo i mezzi per dimostrarlo.

Teorema 2.8. *L/K di Galois finita, $K \subset L, F \subset \Omega$. Allora*

$$\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F) \ , \ [LF : F] = [L : L \cap F] \mid [L : K]$$



Dimostrazione. LF/F é di Galois in quanto traslato di L/K. La mappa

$$\cdot|_L : \mathrm{Gal}(LF/F) \to \mathrm{Gal}(L/L \cap F)$$

é ben definita ed é iniettiva. Vediamo la surgettivitá.
Sia $H = \cdot|_L(\mathrm{Gal}(LF/F))$: dico che H e $\mathrm{Gal}(L/L\cap F)$ fissano lo stesso campo, e quindi sono uguali per la corrispondenza di Galois.
Noto che $H < \mathrm{Gal}(L/L \cap F) \implies L \cap F \subset L^H$. D'altra parte, data $\alpha \in L^H \subset L$, $\forall\ \sigma \in \mathrm{Gal}(LF/F)$ vale $\sigma|_L(\alpha) = \alpha$, ossia $\alpha \in LF^{\mathrm{Gal}(LF/F)} = F$.
Segue che $L^H = L \cap F$, da cui la tesi. □

Teorema 2.9. *Siano $L/K, F/K$ di Galois. Allora*

$$(\cdot|_L, \cdot|_F) : \mathrm{Gal}(LF/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$$

é iniettiva. Se $L \cap F = K$, é bigettiva.
Inoltre, se $L/K, F/K$ sono finite, allora $(\cdot|_L, \cdot|_F)$ bigettiva $\implies L \cap F = K$.

Dimostrazione. LF/K é di Galois in quanto composto di estensioni di Galois. Sicuramente la mappa $(\cdot|_L, \cdot|_F)$ é iniettiva. Supponiamo che $L \cap F = K$ e mostriamo che in tal caso é anche surgettiva.
Siano $\sigma_1 \in \mathrm{Gal}(L/K)$, $\sigma_2 \in \mathrm{Gal}(F/K)$ tali che $\sigma_1|_{L\cap F} = \sigma_2|_{L\cap F}$. Considero $\sigma \in \mathrm{Gal}(LF/K)$ che estende σ_1 e σ_2: allora

$$(\cdot|_L, \cdot|_F)(\mathrm{Gal}(LF/K)) = \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K) \mid \sigma_1|_{L\cap F} = \sigma_2|_{L\cap F}\}$$

Allora $(\cdot|_L, \cdot|_F)$ é surgettiva.
Siano ora $L/K, F/K$ finite. Allora $(\cdot|_L, \cdot|_F)$ é bigettiva $\iff |\mathrm{Gal}(LF/K)| = |\mathrm{Gal}(L/K)| \cdot |\mathrm{Gal}(F/K)| \iff [LF : K] = [L : K] \cdot [F : K] \overset{2.8}{\iff} [F : K] = [F : L \cap F] \iff K = L \cap F$.

□

Lemma 2.10. *Sia $f \in K[x]$ separabile di grado n. Sia $L = \mathrm{cds}_K\{f\} = K(\alpha_1\ ...\ \alpha_n)$ con $\alpha_i \in \overline{K}$. Sia $X = \{\alpha_1\ ...\ \alpha_n\}$. Allora*

$$\cdot|_X : \mathrm{Gal}(L/K) \hookrightarrow \mathcal{S}_n = \mathcal{S}\{X\}$$

Quindi $|\mathrm{Gal}(L/K)| = [L : K] \mid n!$. Inoltre,

$$f \text{ irriducibile} \iff \mathrm{Gal}(L/K) \text{ agisce transitivamente su } X$$

Corollario 2.11. *L/K di Galois, $[L : K] = n$. Allora $\mathrm{Gal}(L/K) < \mathcal{S}_n$.*

Dimostrazione. Per il teorema dell'elemento primitivo (1.43), $L = K(\gamma)$; quindi $L = \mathrm{cds}_K\{\mu_\gamma\}$ e per il lemma sopra si ha la tesi.

□

Definizione 2.12. Un'estensione di Galois si dice **abeliana** (risp. **ciclica**) se il suo gruppo di Galois é un gruppo abeliano (risp. ciclico).

Vediamo quali sono le proprietá dell'*essere abeliana* e dell'*essere ciclica* (prenderme estensioni intermedie sempre di Galois, altrimenti non ha senso parlare di *abeliana* o *ciclica*):

- **torri**:

  $$L/K \text{ abeliana (risp. ciclica)} \implies L/F, F/K \text{ abeliane (risp. cicliche)}$$

  in quanto sottogruppi di un gruppo abeliano/ciclico sono abeliani/ciclici. Tuttavia

  $$L/F, F/K \text{ abeliane (risp. cicliche)} \not\Rightarrow L/K \text{ abeliana (risp. ciclica)}$$

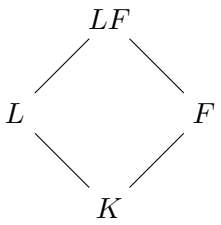
  in quanto non é nemmeno detto che sia normale: si pensi a

  $$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{4})$$

- **shift**:

  $$L/K \text{ abeliana (risp. ciclica)} \implies LF/F \text{ abeliana (risp.ciclica)}$$

  in quanto $\mathrm{Gal}(LF/F) \hookrightarrow \mathrm{Gal}(L/K)$.



- **composto**:

  $$L/K, F/K \text{ abeliane} \implies LF/K \text{ abeliana}$$

  in quanto $\mathrm{Gal}(LF/K) \hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$, mentre le estensioni cicliche non si conservano mai (a meno che una tra L/K e F/K non sia banale).

Esercizio 2.13. Siano $L = \overline{L}$, $\sigma \in \mathrm{Aut}(L)$ e $K = L^{<\sigma>}$. Allora ogni estensione finita di K è ciclica.

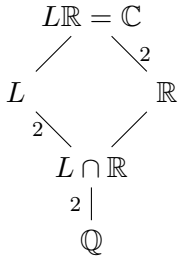
Dimostrazione. Notiamo preliminarmente che L contiene una chiusura algebrica di K. Di conseguenze $\sigma(\overline{K}) = \sigma(\overline{K})$ e $K = \overline{K}^{\langle\sigma\rangle}$. Di conseguenza, $\overline{K}/K$ è algebrico e indotta dall'azione di un gruppo di automorfismi di $\overline{K}$. Per il lemma di Artin 2.3, $\overline{K}/K$ è separabile e normale. Sia ora F un'estensione finita di K e sia $\tilde{F}$ una sua chiusura normale. Se mostriamo che $\tilde{F}/K$ è ciclica, otteniamo la tesi. D'altronde

$$\mathrm{Gal}\left(\tilde{F}\diagup_K\right) = \langle\sigma|_{\tilde{F}}\rangle$$

Infatti $\sigma|_{\tilde{F}}$ è un sottogruppo che fissa solo K e dunque per il teorema di corrispondenza vale l'uguaglianza. □

Esercizio 2.14. Sia $a \in \mathbb{N}$ e sia $K = \mathbb{Q}(\sqrt{-a})$. Allora K non si immerge in un'estensione ciclica di $\mathbb{Q}$ di grado multiplo di 4.

Dimostrazione. Supponiamo per assurdo che esista $L/\mathbb{Q}$ ciclica di grado $4d$ avente come campo intermedio $\mathbb{Q}(\sqrt{-a})$. Possiamo supporre $d = 1$; altrimenti potremmo considerare una sottoestensione di L di grado 4 contenente $\mathbb{Q}(\sqrt{-a})$. Notiamo che $\mathbb{Q}(\sqrt{-a}) \nsubseteq \mathbb{R}$, da cui il diagramma



Dunque $L \cap \mathbb{R}$ è una sottoestensione di grado 2 reale, e dunque distinta da K. Di conseguenza L ammette due sottoestensioni di grado 2 distinte e dunque non può avere gruppo di Galois ciclico, da cui un assurdo. □

2.2 Estensioni ciclotomiche

Sia $f(x) = x^n - 1 \in K[x]$ e sia $U_n = \{\alpha \in \overline{K} \mid \alpha^n = 1\}$: U_n é ciclico in quanto sottogruppo finito moltiplicativo di un campo. Sia $U_n =< \zeta >$.
Se $\mathrm{char}\, K = 0$ oppure $\mathrm{char}\, K = p \nmid n$, allora $|U_n| = n$ e f é separabile. Inoltre, se $K = \mathbb{F}_q$, allora $K(U_n) = \mathbb{F}_{q^d}$ con $d = \min\{h \mid U_n \subset \mathbb{F}_{q^d}^{\times}\} \implies n \mid q^d - 1$ e $d = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} q$.
Se $\mathrm{char}\, K \mid n$ e $n = p^e m$ con $p \nmid m$, allora $f(x) = (x^m - 1)^{p^e}$.

Consideriamo ora $K = \mathbb{Q}$ e $U_n =< \zeta_n >$ con ζ_n una radice n-esima primitiva dell'unitá. Allora $K(U_n) = \mathbb{Q}(\zeta_n)$.

Proposizione 2.15. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *é di Galois. Inoltre,* $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$ *e*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

Dimostrazione. L'estensione è normale in quanto cds di $x^n - 1$ su K. Inoltre, é separabile per il criterio della derivata applicato a $x^n - 1$. Dunque, l'estensione é di Galois.
Sia $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tale che $\sigma(\zeta_n) = \zeta_n^i$ e $\sigma(< \zeta_n >) =< \zeta_n >$. Perché σ sia automorfismo, deve essere $(i, n) = 1$. Ne segue che ho $\phi(n)$ possibili immagini per ζ_n, quindi $[\mathbb{Q}(\zeta_n):\mathbb{Q}] \leq \phi(n)$.
Mi basta ora vedere che $\forall\ i$ coprimo con n si ha $\mu_\zeta(\zeta_n^i) = 0$: per farlo, mostriamo che se a é radice di μ, allora lo é a^p per ogni $p \nmid n$.
Sia $f(x) = x^n - 1 = \mu(x)g(x)$. Se per assurdo $\mu(a^p) \neq 0$, allora $g(a^p) = 0$ e a sarebbe radice di $g(x^p)$: dunque $g(x^p) = \mu(x)g_1(x)$. Riduco tutto modulo p:

$$\overline{\mu} \mid \overline{g(x^p)} = \overline{g(x)}^p \implies (\overline{\mu}, \overline{g}) \neq 1 \implies \overline{f} = x^n - 1 = \overline{\mu g}$$

ossia $\overline{f}$ ha radici multiple (assurdo, per i criterio della derivata).
Ne segue che $\phi(n) \leq [\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg \mu$, e quindi $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$.
Infine, posto $\sigma_i : \zeta_n \mapsto \zeta_n^i$, si dimostra che la mappa

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

tale che $\sigma_i \mapsto [i]$ é un isomorfismo di gruppi.

□

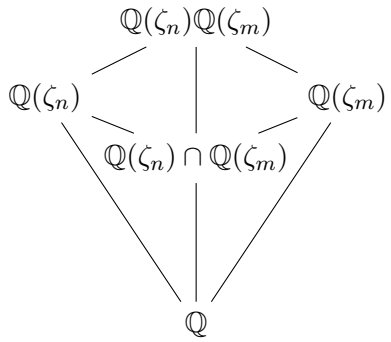
Osservazione.

$$\phi([m,n]) = \frac{\phi(n)\phi(m)}{\phi((m,n))}$$

Si verifica facilmente guardando le potenze dei primi nelle fattorizzazioni.

Proposizione 2.16. *Siano* ζ_n, ζ_m *radici (risp. n-esima ed m-esima) primitive dell'unitá. Allora:*

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

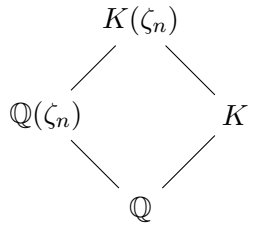


Dimostrazione. Si mostrano le doppie inclusioni, aiutandosi con i gradi delle estensioni.

□

Proposizione 2.17. *Sia $\mathbb{Q} \subset K$. Allora:*

1. $[K(\zeta_n) : K] = d \mid \phi(n)$;
2. μ_{ζ_n} *si fattorizza in* K *come prodotto di* $\frac{\phi(n)}{d}$ *fattori di grado* d.



2.3 Teoria di Galois infinita

Sia L/K un'estensione di Galois *infinita*. Sappiamo che in questo caso il gruppo di Galois non è facilmente calcolabile, in quanto la corrispondenza non vale più nella forma enunciata precedentemente. Vogliamo allora studiare il gruppo di Galois in termini delle sottoestensioni finite. Consideriamo la famiglia

$$\mathcal{L} = \mathcal{L}_{L/K} = \{L_i \mid K \subset L_i \subset L,\ L_i/K \text{ di Galois finita}\}$$

Allora $L = \bigcup_{i \in I} L_i$ e per ogni i si ha la restrizione

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

avente come nucleo $\mathrm{Ker}(\cdot|_{L_i}) = \mathrm{Gal}(L/L_i) \lhd \mathrm{Gal}(L/K)$. Possiamo considerare la mappa

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

L'immagine di ρ sono le successioni coerenti, ossia quelle tali che se $L_i \subset L_j$, allora $\sigma_j|_{L_i} = \sigma_i$. Infatti, per la coerenza, è ben definita l'estensione dei $\sigma_i \in \mathrm{Gal}(L_i/K)$ ad un $\sigma \in \mathrm{Gal}(L/K)$. Inoltre, ρ è iniettiva: se $\rho(\sigma) = (id)_I$, allora per ogni $\alpha \in L$ esiste un indice i tale che $\sigma(\alpha) = \sigma_i(\alpha) = \alpha$, ossia $\sigma = id$.

Vogliamo ora dotare $\mathrm{Gal}(L/K)$ di una topologia. Per questo, utilizziamo l'omomorfismo ρ appena definito. Muniamo ora il gruppo del prodotto della topologia discreta; tramite ρ, possiamo dotare $\mathrm{Gal}(L/K)$ della topologia di sottospazio.

Definizione 2.18. Chiamiamo **topologia di Krull** la topologia indotta da ρ su $\mathrm{Gal}(L/K)$, ossia

$$\mathcal{K} = \{\rho^{-1}(\mathcal{U}_i) \mid \mathcal{U}_i \subset \prod_I \mathrm{Gal}(L_i/K) \text{ aperto}\}$$

Vediamo quindi chi sono gli aperti in $\prod_I \mathrm{Gal}(L_i/K)$: una pre-base è data dagli $\mathcal{U}_i = \prod_j V_j$ con

$$V_j = \mathrm{Gal}(L_j/K) \text{ se } i \neq j,\ V_i = \{\sigma_i\}$$

Dunque, gli aperti sono tutti della forma

$$\rho^{-1}(\prod_j V_j) = (\cdot|_{L_i})^{-1}(\sigma_i) = \tilde{\sigma_i}\,\mathrm{Gal}(L/L_i)$$

(con $\tilde{\sigma_i}$ l'estensione di σ_i a L), ossia sono le classi laterali dei nuclei delle restrizioni $\cdot|_{L_i}$. Allora una pre-base della topologia di Krull su $\mathrm{Gal}(L/K)$ è

$$\{\sigma\,\mathrm{Gal}(L/L_i) \mid \sigma \in \mathrm{Gal}(L/K)\}_{i\in I}$$

Cerchiamo ora una formula per l'intersezione di due aperti della pre-base.

$$\tilde{\sigma_i}\,\mathrm{Gal}(L/L_i) \cap \tilde{\sigma_j}\,\mathrm{Gal}(L/L_j) = \emptyset$$

oppure

$$\tilde{\sigma_i}\,\mathrm{Gal}(L/L_i) \cap \tilde{\sigma_j}\,\mathrm{Gal}(L/L_j) = \bigcup_{r=1}^{n} \tilde{\sigma_r}\,\mathrm{Gal}(L/L_k)$$

con $L_k \subset L_iL_j$. Si osservi che $\sigma_i \in \mathrm{Gal}(L_i/K)$ non ha un'unica estensione a L, ma si estende a $\tilde{\sigma_{i_1}}, \ldots, \tilde{\sigma_{i_m}}$.

Proposizione 2.19. $(\mathrm{Gal}(L/K), \mathcal{K})$ *è un gruppo topologico.*

Dimostrazione. Dobbiamo mostrare che le mappe

$$m : (\sigma, \tau) \mapsto \sigma\tau \qquad\qquad \gamma : \sigma \mapsto \sigma^{-1}$$

sono continue. Devo verificare che le controimmagini di aperti tramite le mappe m e γ sono aperti.

- Sia $\sigma\tau\,\mathrm{Gal}(L/L_k)$ un aperto in $\mathrm{Gal}(L/K)$. Considero $\mathcal{U}_\sigma = \sigma\,\mathrm{Gal}(L/L_k)$ e $\mathcal{U}_\tau = \mathrm{Gal}(L/L_k)$. Ma $m(\mathcal{U}_\sigma, \mathcal{U}_\tau) = \mathcal{U}_\sigma\mathcal{U}_\tau \overset{(*)}{=} \mathcal{U}_{\sigma\tau}$, dove $\overset{(*)}{=}$ é dovuto all'operazione tra classi laterali. Allora $m^{-1}(\sigma\tau\,\mathrm{Gal}(L/L_k)) = \mathcal{U}_\sigma \times \mathcal{U}_\tau$, che é aperto.
- Sia $\sigma^{-1}\,\mathrm{Gal}(L/L_k)$ un aperto in $\mathrm{Gal}(L/K)$ e con considerazioni analoghe si ha $\gamma^{-1}(\sigma^{-1}\,\mathrm{Gal}(L/L_k)) = \sigma\,\mathrm{Gal}(L/L_k)$, che é aperto.

□

Notiamo che una volta definiti gli intorni di 1, gli intorni di $\sigma \in \mathrm{Gal}(L/K)$ sono definiti dalle traslazioni degli intorni di 1. Indichiamo con $\mathcal{I}(x) = \{\mathcal{U} \subset \mathrm{Gal}(L/K) \text{ intorno di } x\}$. Allora una base di $\mathcal{I}(1) = \{\mathrm{Gal}(L/L_i)\}_{i\in I}$, per cui dato $\sigma \in \mathrm{Gal}(L/K)$ si ha

$$\mathcal{I}(\sigma) = \{\sigma\,\mathrm{Gal}(L/L_i)\}_{i\in I}$$

Osservazione. In ogni gruppo topologico, i sottogruppi aperti sono anche chiusi: infatti se $H < G$ é aperto, allora gH è aperto per ogni $g \in G$; ma allora $G = \bigcup_g gH \implies G - H = \bigcup_{g\neq id} gH$, che é aperto in quanto unione di aperti. Ne segue che H è anche chiuso. In particolare, i $\mathrm{Gal}(L/L_i)$ sono aperti e chiusi.

Ricordiamo ora qualche definizione di Topologia. Uno spazio topologico è *di Hausdorff* (o $T2$) se per ogni coppia di punti distinti esistono due intorni disgiunti che li contengono. Uno spazio topologico è *compatto* se ogni ricoprimento di aperti ammette un sottoricoprimento finito. Uno spazio topologico è *totalmente sconnesso* se le sue componenti connesse sono tutte e sole i punti.

Lemma 2.20. $(\mathrm{Gal}(L/K), \mathcal{K})$ *è di Hausdorff, compatto e totalmente sconnesso.*

Dimostrazione.

- Siano $\sigma \neq \tau \in \mathrm{Gal}(L/K)$: in quanto distinti su L, esiste un indice i tale che $\sigma|_{L_i} \neq \tau|_{L_i}$. Di conseguenza $\sigma\,\mathrm{Gal}(L/L_i) \cap \tau\,\mathrm{Gal}(L/L_i) = \emptyset$ (sono due aperti disgiunti che separano σ e τ). Segue che $\mathrm{Gal}(L/K)$ è T2.

- $\mathrm{Gal}(L_i/K)$ è compatto con la topologia discreta in quanto finito, dunque lo è anche $\prod \mathrm{Gal}(L_i/K)$ (prodotto di compatti è compatto). Basta allora mostrare che $\rho(\mathrm{Gal}(L/K))$ è chiuso: in tal caso $\mathrm{Gal}(L/K)$ sarebbe chiuso in un compatto e dunque compatto. Sia $(\sigma_i)_i$ una successione non coerente. Allora esistono i, j tali che $L_i \subset L_j$ ma $\sigma_j|_{L_i} \neq \sigma_i$. Consideriamo allora $\prod V_h$ con

  $$V_h = \mathrm{Gal}(L_h/K) \text{ se } h \neq i, j,\ V_i = \{\sigma_i\},\ V_j = \{\sigma_j\}$$

  Questo è un aperto ed è un intorno di $(\sigma_i)_i$ formato da successioni non coerenti. Ne segue che $\mathrm{Gal}(L/K)$ è chiuso in $\prod \mathrm{Gal}(L_i/K)$.

- $\prod \mathrm{Gal}(L_i/K)$ è totalmente sconnesso in quanto prodotto di gruppi topologici discreti, dunque $(\mathrm{Gal}(L/K), \mathcal{K})$ è totalmente sconnesso.

□

Lemma 2.21. *Sia $H < \mathrm{Gal}(L/K)$ e sia $\overline{H}$ la sua chiusura topologica. Allora $\mathrm{Gal}(L/L^H) = \overline{H}$.*

Dimostrazione. $\supseteq$ Siano $F = L^H$ e $\mathcal{L} = \{L_i\}_{i\in I}$ l'insieme delle sottoestensioni di L/K finite e di Galois su K. Detta res_i la mappa di restrizione da $\mathrm{Gal}(L/K)$ a $\mathrm{Gal}(L_i/K)$, chiamiamo $H_i = res_i(H)$ e notiamo che $L_i^{H_i} = L_i \cap F$. Dato che su $\mathrm{Gal}(L_i/K)$ si ha la topologia discreta, H_i è chiuso e dunque

$$H' = \bigcap_{i\in I} res_i^{-1}(H_i)$$

è un sottogruppo chiuso di $\mathrm{Gal}(L/K)$ in quanto intersezione di chiusi. Chiaramente $L^{H'} = L^H$ in quanto $res_i(H) = res_i(H')$ e $F = \cup(L_i^{H_i})$. Inoltre, H' è il più grande sottogruppo di $\mathrm{Gal}(L/K)$ che fissa F per costruzione, ossia $H' = \mathrm{Gal}(L/F)$. Di conseguenza $\overline{H} \subseteq \mathrm{Gal}(L/F)$.

$\subseteq$ Sia $\sigma \in H'$ e sia E una sottoestensione di Galois finita di L/F. La restrizione

$$res_i \colon H \longrightarrow \mathrm{Gal}\left(E/F\right)$$

è surgettiva e dunque esiste $\tau \in H$ tale che $\tau|_E = \sigma|_E$. Dunque $\tau \in H \cap \sigma\,\mathrm{Gal}(L/F)$, ossia ogni intorno di σ interseca H. Di conseguenza $\sigma \in \overline{H}$, da cui la tesi.

□

Generalizziamo ora la corrispondenza di Galois alle estensioni infinite.

Teorema 2.22 (Corrispondenza di Galois - parte II)**.** *Sia L/K un'estensione di Galois e sia $G = \mathrm{Gal}(L/K)$. Allora esistono due mappe*

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

che sono bigettive e l'una inversa dell'altra.

Dimostrazione. Dal teorema di corrispondenza nel caso finito 2.5, segue che $\phi \circ \psi = id$. Per il lemma precedente ψ è surgettiva, e quindi vale anche $\psi \circ \phi = id$, da cui la tesi. □

Proposizione 2.23. *I sottogruppi aperti di $\mathrm{Gal}(L/K)$ corrispondono alle sottoestensioni finite F/K.*

Dimostrazione. Sia H un sottogruppo aperto (e dunque chiuso) di $G = Gal(L/K)$. Dato che $G = \sqcup \sigma H$ e G è compatto, le classi laterali di H in G sono in numero finito. Ne segue che i sottogruppi aperti di G hanno indice finito. Consideriamo ora la mappa

$$\begin{array}{rccc} \varphi\colon & {}^{G}\!/_{H} & \longrightarrow & \mathrm{Hom}_K(L, \overline{K}) \\ & \sigma H & \longmapsto & \sigma|_L \end{array}$$

φ individua una corrispondenza biunivoca tra le classi laterali di H e le immersioni, da cui $[L^H : K] = \left|{}^{G}\!/_{H}\right|$. □

2.4 Gruppi profiniti, interi p-adici e $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$

Vogliamo classificare i gruppi di Galois infiniti come *gruppi profiniti* e caratterizzarli come *limiti proiettivi*.

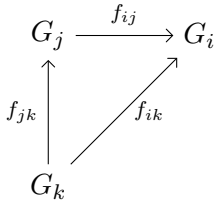
Definizione 2.24. Un gruppo topologico G si dice **gruppo profinito** se é di Hausdorff, compatto e ammette una base di intorni di 1 fatta da sottogruppi normali.

Dalla definizione e da quanto detto (e dimostrato) fin'ora, segue che i gruppi di Galois sono gruppi profiniti. Inoltre, tutti i gruppi finiti con la topologia discreta sono profiniti.

Definizione 2.25. Un insieme di indici I con ordine parziale $\leq$ si dice **diretto** se

$$\forall i, j \in I \quad \exists k \in I \ \text{ tale che } \ i, j \leq k$$

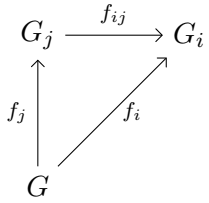
Definizione 2.26. Sia I diretto. Definisco **sistema proiettivo** su I una famiglia $\{G_i, f_{ij}\}_{i,j \in I}$ con G_i oggetti in una categoria e $\forall\, i < j,\ f_{ij} : G_j \to G_i$ morfismo della categoria tale che $f_{ii} = id\ \forall i$ e $\forall\, i \leq j \leq k$ si ha il diagramma commutativo



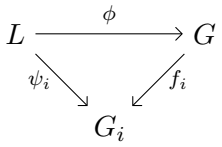
Definizione 2.27. Dato il sistema proiettivo $\{G_i, f_{ij}\}_{i \leq j}$, sia

$$\{G = \varprojlim G_i, f_i\}$$

l'elemento universale della categoria per il sistema, dove $f_i : G \to G_i$ ha la proprietá ($\mathcal{P}$) "$\forall\ i \leq j$ fa commutare il diagramma"



Dico che $\{G, f_i\}$ é il **limite proiettivo** del sistema proiettivo dato se, $\forall\ \{L, \psi_i\}$ per cui vale $\mathcal{P}$, esiste $\phi : L \to G$ che $\forall\ i$ fa commutare il diagramma



Si dimostra che tale oggetto universale é unico.
Consideriamo ora la categoria dei gruppi topologici con morfismi gli omomorfismi continui. L'elemento universale é

$$\varprojlim G_i = \{\{\sigma_i\} \in \prod G_i \mid f_{ij}(\sigma_j) = \sigma_i\ \forall\ i \leq j\}$$

Osservazione. Poiché

$$\mathrm{Gal}(L/K) = \{\{\sigma_i\} \in \mathrm{Gal}(L_i/K) \text{ coerenti} \mid L_i/K \text{ di Galois finita}\}$$

si ha

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

con $L_i \subset L_j$ e $f_{ij} = \cdot|_{L_i}$ per ogni $i \leq j$.

Osservazione.

$$G_i\ T2 \implies \varprojlim G_i\ T2 \text{ e chiuso nel prodotto dei } G_i$$

Vale il seguente risultato (che non dimostriamo):

Teorema 2.28. *Ogni gruppo profinito é il limite proiettivo di una certa famiglia di gruppi finiti con la topologia discreta.*
In particolare:

- *se G é profinito e $\{N_i \triangleleft G$ aperti$\}$, allora G e $\varprojlim(G/N_i)$ sono isomorfi e omeomorfi.*
- *se $\{G_i, f_{ij}\}$ é un sistema proiettivo di gruppi finiti con la topologia discreta, allora $G = \varprojlim G_i$ é gruppo profinito.*

Esempio (Interi p-adici)**.** Date $\pi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ le proiezioni canoniche per $n \leq m$, $\{\mathbb{Z}/p^n\mathbb{Z}, \pi_{nm}\}$ é un sistema proiettivo.
Definisco **anello degli interi p-adici** l'anello

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

i cui elementi (detti *interi p-adici*) sono del tipo

$$(a_0,\ a_0 + pa_1,\ a_0 + pa_1 + p^2a_2,\ \dots\ )$$

con $\sum^N p^i a_i \in \mathbb{Z}/p^{N+1}\mathbb{Z}$ e li identifichiamo con le serie $\sum_{i\geq 0} a_i p^i$.

Esempio. Date $\pi_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le proiezioni canoniche per $n \leq m$, $\{\mathbb{Z}/n\mathbb{Z}, \pi_{nm}\}$ é un sistema proiettivo. Denotiamo

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \varprojlim \mathbb{Z}/n!\mathbb{Z}$$

Proposizione 2.29. *$\hat{\mathbb{Z}}$ e $\prod_p \mathbb{Z}_p$ sono isomorfi come gruppi topologici.*

Dimostrazione. Consideriamo l'omomorfismo di gruppi

$$\begin{array}{rccc} \phi\colon & \hat{\mathbb{Z}} & \longrightarrow & \prod_p \mathbb{Z}_p \\ & \{\sigma_i\}_{i\in\mathbb{N}} & \longmapsto & \{\{\sigma_{p^n}\}_{n\in\mathbb{N}}\}_p \end{array}$$

ϕ è ben definita in quanto successioni coerenti vanno in successioni coerenti. Mostriamo che ϕ è iniettiva. Sia $\{\sigma_n\}$ tale che $\phi(\{\sigma_n\}) = \{\{0\}\}$, ossia $\sigma_{p^n} = 0$ per ogni p primo e $n \in \mathbb{N}$. Mostriamo che $\sigma_m = 0$ per ogni m. Fissato $m \in \mathbb{N}$, sia $m = p_1^{e_1} \dots p_r^{e_r}$. Poiché $\sigma_{p_i^{e_i}} = 0$ per ogni i e $\sigma_m \equiv \sigma_{p_i^{e_i}} \equiv 0 \pmod{p_i^{e_i}}$ per ogni i, per il teorema cinese del resto si ha $\sigma_m \equiv 0 \pmod{m}$. Mostriamo ora che ϕ è surgettiva. Sia $\{\{\sigma_{p^i}\}_i\}_p$; cerchiamo $\{\sigma_n\}$ tale che, se $n = p_1^{e_1} \dots p_r^{e_r}$, $\sigma_n \equiv \sigma_{p_i^{e_i}} \pmod{p_i^{e_i}}$ per ogni indice i. Per il teorema cinese del resto questo sistema ha soluzione e la soluzione è coerente. Notiamo che ϕ è un omeomorfismo: infatti intorni di $\{\sigma_n\}$ vanno in intorni di $\phi(\{\sigma_n\})$. □

Determiniamo ora il gruppo di Galois assoluto dei campi finiti:

Proposizione 2.30. $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$.

Dimostrazione. Consideriamo $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^i}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z}$ con omomorfismi le restrizioni π'_{nm} e il diagramma

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

che commuta. Quindi $\varprojlim\{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p), \pi'_{nm}\} \cong \varprojlim\{\mathbb{Z}/n\mathbb{Z}, \pi_{nm}\}$ e quest'ultimo è proprio $\hat{\mathbb{Z}}$. □

Proposizione 2.31. *Sia $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ con p_i primi o $p_i = -1$ (distinti). Allora*

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$$

Inoltre, se $L = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\} \cup \{-1\})$, vale

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \prod^{\infty} \mathbb{Z}/2\mathbb{Z}$$

Studiamo ora tutte le estensioni algebriche di $\mathbb{F}_p$ e i sottogruppi del suo gruppo di Galois assoluto (che abbiamo appena visto essere $\hat{\mathbb{Z}}$).
Sia $q \in \mathbb{Z}$ primo e sia $L_q = \bigcup_{n\geq 0} \mathbb{F}_{p^{q^n}}$. Questa sottoestensione coincide con il sottogruppo $\mathbb{Z}_q$.

$$\begin{array}{cc} \overline{\mathbb{F}_p} & \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}} \\ \infty \,\big|\, & \big| \\ L_q & \mathrm{Gal}(L_q/\mathbb{F}_p) \cong \mathbb{Z}_q \\ \infty \,\big|\, & \big| \\ \mathbb{F}_p & \{id\} \end{array}$$

Studiamo dapprima le estensioni intermedie F di $L_q/\mathbb{F}_p$. Definiamo

$$q^{\overline{n}} = \sup\{[\mathbb{F}_p(x) : \mathbb{F}_p] \mid x \in F\}$$

con $\overline{n} \in \mathbb{N} \cup \{\infty\}$. Se $\overline{n} < \infty$, $F = \mathbb{F}_{p^{q^{\overline{n}}}}$. Infatti sicuramente $\mathbb{F}_{p^{q^{\overline{n}}}} \subset F$ per definizione di $q^{\overline{n}}$; inoltre, trattandosi di estensioni separabili finite, per il teorema dell'elemento primitivo 1.43 si ha l'altra inclusione. Se invece $\overline{n} = \infty$, allora $\mathbb{F}_{p^{q^n}} \subseteq \mathbb{F}_{p^{q^{\overline{n}}}}$ per ogni $n \in \mathbb{N}$. Dato che l'unione dei primi è proprio L_q, si ha l'uguaglianza. Per quanto riguarda i sottogruppi, sappiamo che $\mathrm{Gal}(L_q/\mathbb{F}_p) \cong \mathbb{Z}_q = \overline{\langle\phi\rangle}$, dove ϕ è il Frobenius di $\overline{\mathbb{F}_p}$ ristretto a L_q. Per quanto visto, il sottogruppo corrispondente a F è $\langle\phi^{q^{\overline{n}}}\rangle$.

$$\langle\phi^{q^{\overline{n}}}\rangle = \overline{\langle\phi^{q^{\overline{n}}}\rangle} \overset{2.21}{=} \mathrm{Gal}(L_q/L_q^{\langle\phi^{q^{\overline{n}}}\rangle}) \cong q^{\overline{n}}\mathbb{Z}_q$$

Abbiamo dimostrato che i sottogruppi chiusi di $\mathbb{Z}_q$ sono del tipo $\mathrm{Gal}(L_q/\mathbb{F}_{p^{q^{n_F}}})$, e dalla corrispondenza di Galois (2.22) sappiamo che sono in corrispondenza con le sottoestensioni di L_q.
Generalizziamo ora questo ragionamento a tutte le sottoestensioni di $\overline{\mathbb{F}}_p$. Sia $\mathbb{F}_p \subset K \subset \overline{\mathbb{F}}_p$. Consideriamo $K \cap L_q = K^{(q)} \subset L_q$. Per quanto visto prima sappiamo che $K^{(q)} = \mathbb{F}_{p^{q^{n_q}}}$ e notiamo che

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

e si ha il gruppo di Galois

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

che è intersezione di chiusi di $\hat{\mathbb{Z}}$, dunque è un chiuso di $\hat{\mathbb{Z}}$.

Cerchiamo di riformulare quanto appena ottenuto in termini di gruppi e numeri naturali.

Definizione 2.32. Definiamo **numero di Steinitz** (o **supernaturale**) un valore del tipo

$$a = \prod_q q^{n_q}$$

con $n_q \in \mathbb{N} \cup \{0\}$.

Allora i sottogruppi chiusi di $\hat{\mathbb{Z}}$ sono quelli del tipo $a\hat{\mathbb{Z}}$ con a supernaturale. Osserviamo che se $q \neq l$ si ha $q\mathbb{Z}_l = \mathbb{Z}_l$, e quindi

$$a\hat{\mathbb{Z}} = \prod_q a\mathbb{Z}_q = \prod_q q^{n_q}\mathbb{Z}_q$$

Dunque abbiamo visto il seguente:

Teorema 2.33. *La mappa $a \mapsto a\hat{\mathbb{Z}}$ è una corrispondenza biunivoca tra i supernaturali e i sottogruppi chiusi di $\hat{\mathbb{Z}}$.*

2.5 Problema inverso di Galois: realizzabilitá su $\mathbb{Q}$

Definizione 2.34. Diciamo che un gruppo G **si realizza** su un campo K se esiste un sovracampo F di K tale che $\mathrm{Gal}(F/K) = G$.

Mostriamo che i gruppi abeliani si realizzano su $\mathbb{Q}$; per questo, utilizziamo il seguente:

Teorema 2.35 (Dirichlet)**.** *Sia $n \in \mathbb{N}$. Allora esistono infiniti primi p tali che $p \equiv 1 \pmod{n}$.*

Teorema 2.36. *I gruppi abeliani finiti si realizzano su $\mathbb{Q}$.*

Dimostrazione. Separiamo la dimostrazione in due parti:

- Se $G = \mathbb{Z}/n\mathbb{Z}$ è ciclico, per il teorema di Dirichlet esiste un primo p tale che $p \equiv 1 \pmod{n}$. Dunque $p - 1 = nd$ e $\mathbb{Z}/(p-1)\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ ha un quoziente isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

- Se G è un gruppo abeliano finito, per il teorema di struttura si ha

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

Per ogni indice i, possiamo scegliere un primo p_i tale che $p_i \equiv 1 \pmod{n_i}$ e $p_i \neq p_j$, in quanto per il teorema di Dirichlet tali primi sono infiniti. Di conseguenza, detto $m = \prod p_i$, G è un quoziente del gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, da cui la tesi.

□

Si può dimostrare che $\mathbb{Z}$ non si realizza su $\mathbb{Q}$ in quanto non è un gruppo profinito, ma non lo vedremo. Da questo si deduce che il teorema non si estende ai gruppi abeliani infiniti.

Definizione 2.37. Definiamo **chiusura abeliana** di $\mathbb{Q}$

$$\mathbb{Q}^{ab} = \bigcup_{\mathbb{Q}\subset K \text{ abeliana}} K$$

Notiamo che $\mathbb{Q}^{ab}$ coincide con la massima sottoestensione di $\overline{\mathbb{Q}}$ abeliana su $\mathbb{Q}$. Dalla teoria di Galois sappiamo che $\mathbb{Q}^{ab}$ è fissata dal minimo sottogruppo chiuso N di $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tale che G/N è abeliano, ossia $N = \overline{[G,G]}$, dove $[G,G]$ è il gruppo dei commutatori di G. Questo segue dal fatto che G/N è abeliano se e solo se $[G,G] \subset N$. Useremo il seguente:

Teorema 2.38 (Kronecker-Weber)**.** *Ogni estensione abeliana finita di $\mathbb{Q}$ è contenuta in una estensione ciclotomica.*

Proposizione 2.39. *Sia $\mathbb{Q}^{ab}$ la chiusura abeliana di $\mathbb{Q}$. Allora*

$$\mathrm{Gal}\left(\mathbb{Q}^{ab}/\mathbb{Q}\right) \cong \hat{\mathbb{Z}}^\times$$

Dimostrazione. Dal teorema di Kronecker-Weber sappiamo che ogni estensione abeliana è contenuta in una estensione ciclotomica. Di conseguenza $\mathbb{Q}^{ab} = \bigcup \mathbb{Q}(\zeta_n)$, per cui

$$\mathrm{Gal}\left(\mathbb{Q}^{ab}/\mathbb{Q}\right) = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n | n \in \mathbb{N})/\mathbb{Q}\right) \overset{(*)}{=} \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$$

dove $(*)$ segue dal fatto che l'insieme è filtrante. □

Realizzabilità di S_n Sia K un campo e siano $T_1, \ldots, T_n$ indeterminate. Sia $L = K(T_1, \ldots, T_n)$. Consideriamo l'azione di $\mathcal{S}_n$ su $\{T_1 ... T_n\}$

$$\sigma\left(\frac{f(T_1 ... T_n)}{g(T_1 ... T_n)}\right) = \frac{f(T_{\sigma(1)} ... T_{\sigma(n)})}{g(T_{\sigma(1)} ... T_{\sigma(n)})}$$

per cui $\mathcal{S}_n \hookrightarrow \mathrm{Aut}(L)$. Per il lemma di Artin (2.3), posto $F = L^{\mathcal{S}_n}$, L/F è di Galois con $\mathrm{Gal}(L/F) \cong \mathcal{S}_n$. In realtà possiamo dire chi sono i generatori di $L^{\mathcal{S}_n}$ su K: $L^{\mathcal{S}_n}$ è il campo delle funzioni simmetriche nelle variabili $\{T_i\}$, come risulta dal seguente teorema:

Teorema 2.40. *Sia $L = K(T_1, \dots, T_n)$ e siano $s_1, \dots, s_n$ le funzioni simmetriche elementari in $T_1, \dots, T_n$. Allora:*

1. *$L^{\mathcal{S}_n} = K(s_1, \dots, s_n)$;*
2. *$s_1, \dots, s_n$ sono algebricamente indipendenti.*

Dimostrazione.

1. Sappiamo che $[L : L^{\mathcal{S}_n}] = n!$. Consideriamo il polinomio

$$p(x) = \prod(x - T_i) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \in K(s_1, \dots, s_n)[x]$$

Le radici di p sono le indeterminate T_i e dunque $K(T_1, \dots, T_n)$ è il campo di spezzamento di p. Allora $[K(T_1, \dots, T_n) : K(s_1, \dots, s_n)] \mid n!$ e dunque

$$K(s_1, \dots, s_n) \subseteq L^{\mathcal{S}_n} \overset{n!}{\subseteq} L$$

Per motivi di grado, $L^{\mathcal{S}_n} = K(s_1, \dots, s_n)$.

2. Si considerino le indeterminate $X_1, \dots, X_n$ e siano $t_1, \dots, t_n$ le radici di $f(y) = \sum(-1)^k X_k y^k \in K(X_1, \dots, X_n)[y]$ in una chiusura algebrica fissata. Consideriamo l'omomorfismo di valutazione

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

Notiamo che è ben definito poichè $\{T_i\}$ sono algebricamente indipendenti. Si ha che $\varphi(s_i) = X_i$; le X_i sono algebricamente indipendenti e dunque lo sono le s_i. Se infatti le s_i fossero algebricamente dipendenti su K, esisterebbe un polinomio $p \in K(Y_1, \dots, Y_n)$ tale che $p(s_1, \dots, s_n) = 0$, da cui

$$p(s_1, \dots, s_n) = 0 \Longrightarrow \varphi(p(s_1, \dots, s_n)) = 0 \Longrightarrow p(X_1, \dots, X_n) = 0$$

□

Vogliamo ora dimostrare che $\mathcal{S}_n$ si realizza come gruppo di Galois su $\mathbb{Q}$. Per farlo, abbiamo bisogno del teorema di irriducibilità di Hilbert, che enunciamo senza dimostrazione:

Teorema 2.41 (Irriducibilità di Hilbert)**.** *Sia $f(T_1, \dots, T_n, X_1, \dots, X_r) \in \mathbb{Q}[T_1, \dots, T_n, X_1, \dots, X_r]$ 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 2.42. *$\mathcal{S}_n$ si realizza su $\mathbb{Q}$.*

Dimostrazione. Sia $L = \mathbb{Q}(T_1, \ldots, T_n)$ e $K = \mathbb{Q}(s_1, \ldots, s_n)$. Dato che l'estensione L/K è finita e separabile, per il teorema dell'elemento primitivo esiste un elemento Y della forma

$$Y = \sum_{i=1}^{n} \alpha_i T_i \quad \text{con } \alpha_i \in \mathbb{Q}$$

tale che $L = K(Y)$. Sia $\mu \in K[t]$ il polinomio minimo di Y su K; notiamo che per la scelta effettuata di Y, $\mu \in \mathbb{Q}[s_1, \ldots, s_n, t]$. Poiché gli s_i sono algebricamente indipendenti, per il teorema di irriducibilità di Hilbert esistono $a_1, \ldots, a_n \in \mathbb{Q}$ tali che $\overline{\mu}(t) = \mu(a_1, \ldots, a_n, t)$ sia irriducibile in $\mathbb{Q}[t]$. Sia $\overline{\alpha}$ una radice di $\overline{\mu}$.
Mostriamo che $\mathbb{Q}(\overline{\alpha})/\mathbb{Q}$ è di Galois con gruppo di Galois $\mathcal{S}_n$. μ ha grado $n!$ nella variabile t e dunque lo stesso vale per $\overline{\mu}$, in quanto μ è monico nella t. Ne segue che $[\mathbb{Q}(\overline{\alpha}) : \mathbb{Q}] = n!$. Consideriamo ora il polinomio $p(x) = x^n - a_1 x^{n-1} + ... + (-1)^n a_n$; questo coincide con l'immagine del polinomio $q(x) = x^n - s_1 x^{n-1} + ... + (-1)^n a_n$ tramite l'estensione della valutazione all'anello dei polinomi. p ha radici $t_1, \ldots, t_n$ in $\overline{\mathbb{Q}}$ (che "corrispondono" dunque alle T_i) e si ha che $\mathbb{Q} \subset \mathbb{Q}(\overline{\alpha}) \subset \mathbb{Q}(t_1, \ldots, t_n)$. Infatti α corrisponde alla valutazione in uno dei t_i di uno dei coniugati di Y. Ma $\mathbb{Q}(t_1, \ldots, t_n)$ è il campo di spezzamento di p su $\mathbb{Q}$ e p ha grado n: dunque $\mathbb{Q}(t_1, \ldots, t_n)/\mathbb{Q}$ è di Galois e $\mathrm{Gal}(\mathbb{Q}(t_1, \ldots, t_n)/\mathbb{Q}) < \mathcal{S}_n$. Per motivi di grado, si ha $\mathbb{Q}(t_1, \ldots, t_n) = \mathbb{Q}(\overline{\alpha})$ e $\mathrm{Gal}(\mathbb{Q}(\overline{\alpha})/\mathbb{Q}) \cong \mathcal{S}_n$. □

2.6 Discriminante, norma e traccia

Lemma 2.43. *Siano $f, g \in K[x]$ con $\partial f = n$, $\partial g = m$. Allora*

$$(f, g) \neq 1 \iff \exists h, k \in K[x] - \{0\},\ \partial h < m, \partial k < n \text{ tali che } fh = gk$$

Ricordiamo brevemente alcune proprietà del risultante di due polinomi. Siano $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j \in K[x]$. Consideriamo la matrice $Syl(f, g)$, ossia la *matrice di Sylvester* di f e g.

Definizione 2.44. Definiamo **risultante** di f e g

$$R(f, g) = \det Syl(f, g)$$

Valgono le seguenti proprietà:

1. $R(f, g) = 0 \iff (f, g) \neq 1$;
2. $R(f, g) \in \mathbb{Z}[a_i, b_j]$ è omogeneo;
3. Per ogni $f, g \in K[x]$ esistono $h, k \in \mathbb{Z}[a_i, b_j][x]$ con $\deg h < \deg g$, $\deg k < \deg f$ tali che $R(f, g) = fh + gk$;

4. se $f = a\sum^n(x-\alpha_i)$ e $g = b\sum^m(x-\beta_j)$, allora

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

5. $R_y(\mu_\alpha(y), \mu_\beta(x+y))$ si annulla in $\alpha - \beta$;

6. $R_y(\mu_{\frac{1}{\alpha}}(y), \mu_\beta(xy))$ si annulla in $\alpha\beta$.

Introduciamo ora il concetto di discriminante di un polinomio.

Definizione 2.45. Sia $f \in K[x]$ di grado $n \geq 1$, $f = a\prod_{i=1}^n(x-\alpha_i)$. Definisco **discriminante** di f

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

Si osservi che $a^{2(n-1)}$ fa sì che $\operatorname{disc}(f) \in \mathbb{Z}[\operatorname{coeff}(f)]$, altrimenti servirebbe $\mathbb{Q}$.

Proposizione 2.46. $R(f,f') = (-1)^{\frac{n(n-1)}{2}} a \operatorname{disc}(f)$.

Esempio. Dalla precedente proposizione si ottiene:

- Se $f(x) = ax^2 + bx + c$, allora $\operatorname{disc}(f) = b^2 - 4ac$;
- Se $f(x) = x^3 + ax + b$, allora $\operatorname{disc}(f) = -4a^3 - 27b^2$;
- $\operatorname{disc}(f) = 0 \iff (f,f') \neq 1 \iff f$ ha fattori multipli.

Vogliamo ora capire come agisce il gruppo di Galois G del campo di spezzamento di un polinomio f sul discriminante e sulla sua radice $\sqrt{\Delta_f}$. Innanzitutto notiamo che se $f \in K[x]$ allora $\Delta_f \in K$. Date $\alpha_1, \ldots, \alpha_n$ le radici di f, definiamo

$$\delta \coloneqq \prod_{i<j}(\alpha_i - \alpha_j)$$

Allora $\operatorname{disc}(f) = a^{2(n-1)}\delta^2 \in K$ e $\delta \in K(\alpha_1, \ldots, \alpha_n)$. Notiamo che $G = \operatorname{Gal}(K(\alpha_1, \ldots, \alpha_n)/K) < \mathcal{S}_n$. Inoltre, $\delta \in K$ se e solo se $\delta \in \operatorname{Fix} G$. Se agiamo su δ con $\mathcal{S}_n$

$$\mathcal{S}_n \to \mathcal{S}(\alpha_1, \ldots, \alpha_n)$$

si ha che le permutazioni pari fissano δ, mentre quelle dispari gli cambiano il segno, ossia

$$\sigma(\delta) = \delta \iff \sigma \in \mathcal{A}_n$$

Segue il seguente risultato:

Proposizione 2.47. *Sia $f \in K[x]$ irriducibile, $\partial f = n$ e sia $L = \mathrm{cds}_K(f)$. Allora*

$$\mathrm{Gal}(L/K) < \mathcal{A}_n \iff \delta \in K$$

Dimostrazione. Basta notare che

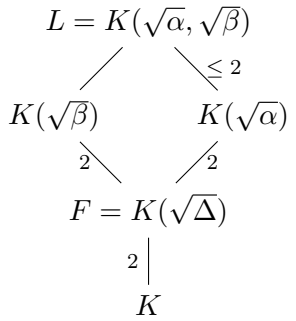
$$\begin{aligned} \delta \in K &\iff \forall\, \sigma \in \mathrm{Gal}(L/K),\ \sigma(\delta) = \delta \\ &\iff \mathrm{Gal}(L/K) < \mathcal{A}_n \end{aligned}$$

□

Esempio (Polinomi di grado 3)**.** Se $f \in K[x]$, $\partial f = 3$ e $L = \mathrm{cds}_K(f)$, allora

- $\mathrm{disc}(f) \notin K^2 \iff \mathrm{Gal}(L/K) \cong \mathcal{S}_3$;
- $\mathrm{disc}(f) \in K^2 \iff \mathrm{Gal}(L/K) \cong \mathcal{A}_3$.

Esempio (Polinomi biquadratici)**.** Posto $\mathrm{char}\, K \neq 2$, consideriamo $f(x) = x^4 + ax^2 + b \in K[x]$ irriducibile e sia L il suo campo di spezzamento. Classifichiamo i possibili gruppi di Galois dell'equazione. Sappiamo che $\mathrm{Gal}(L/K) < \mathcal{S}_4$. Poniamo $g(x) = x^2 + ax + b$ e siano α, β le sue radici: allora le radici di f sono $\pm\sqrt{\alpha}, \pm\sqrt{\beta}$ e quindi $L = K(\sqrt{\alpha}, \sqrt{\beta})$. Consideriamo il diagramma



dove i gradi scritti seguono dall'irriducibilità di f (e dunque di g) e dove $\Delta = \Delta_g$. Ne segue che $[L : K] = 4$ oppure $[L : K] = 8$. Notiamo che

$$[L : K] = 4 \iff F(\sqrt{\alpha}) = F(\sqrt{\beta}) \iff \alpha\beta = b \in F^2$$

Dunque, se $b \notin F^2$, allora $[L : K] = 8$ e $\mathrm{Gal}(L/K)$ è un sottogruppo di cardinalità 8 di $\mathcal{S}_4$, ossia $\mathrm{Gal}(L/K) \cong D_4$. Supponiamo ora che $b \in F^2$, ossia $[L : K] = 4$. Abbiamo due possibilità

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z} \qquad\qquad \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Notiamo che il discriminante di f è

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

e di conseguenza

- se $b \notin K^2$, allora $\mathrm{Gal}(L/K) \nsubseteq \mathcal{A}_4$ e dunque $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$, in quanto G deve essere transitivo e ogni altro sottogruppo di S_4 di cardinalità 4 non contenuto in A_4 non lo è;
- se $b \in K^2$, allora $\mathrm{Gal}(L/K) < \mathcal{A}_4$ e dunque $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Riassumendo,

$$\mathrm{Gal}(L/K) \cong \begin{cases} D_4 & \text{se } b \notin K(\sqrt{\Delta})^2 \\ \mathbb{Z}/4\mathbb{Z} & \text{se } b \in K(\sqrt{\Delta})^2,\ b \notin K^2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{se } b \in K^2 \end{cases}$$

Prima di parlare di traccia e norma di un'estensione finita di campi, introduciamo il concetto di carattere e vediamo un risultato (dovuto ad Emil Artin) che ci tornerà utile.

Definizione 2.48. Siano G un gruppo e K un campo. Definiamo **carattere** un omomorfismo

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

Notiamo che se χ_1, χ_2 sono caratteri, il prodotto $\chi_1 \cdot \chi_2$ definito da $\chi_1 \cdot \chi_2(g) = \chi_1(g)\chi_2(g)$ è ancora un carattere. Notiamo che lo stesso non vale per la somma (la somma di caratteri non è un carattere).

Teorema 2.49 (Indipendenza dei caratteri, Artin)**.** *Caratteri distinti sono sempre linearmente indipendenti su K.*

Dimostrazione. Sia n il minimo intero positivo per cui esiste una combinazione lineare nulla non banale

$$a_1\chi_1 + a_2\chi_2 ... + a_n\chi_n = 0 \tag{2.1}$$

Poiché per ipotesi i caratteri sono distinti, esiste $h \in G$ tale che $\chi_1(h) \neq \chi_2(h)$. Moltiplicando allora la 2.1 per $\chi_1(h)$ otteniamo

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_1(h) + ... + a_n\chi_n(g)\chi_1(h) = 0 \tag{2.2}$$

Dato che l'equazione 2.1 vale per ogni $g \in G$, possiamo valutarla in gh

$$a_1\chi_1(hg) + a_2\chi_2(hg) ... + a_n\chi_n(hg) = 0 \tag{2.3}$$

Sottraendo la 2.3 alla 2.2 si ha

$$\sum_{i \neq 1} a_i(\chi_1(h) - \chi_i(h))\chi_i(g) = 0$$

Ma $\chi_1 \neq \chi_2$, quindi $\chi_2, \ldots, \chi_n$ sono $n-1$ caratteri distinti linearmente dipendenti, contro la minimalità di n, da cui un assurdo. □

Definizione 2.50. Sia L/K un'estensione finita e sia $\alpha \in L$. Sia

$$\begin{array}{rccc} \phi_\alpha \colon & L & \longrightarrow & L \\ & \gamma & \longmapsto & \alpha\gamma \end{array}$$

Definiamo **traccia** di α la traccia dell'applicazione lineare

$$\mathrm{Tr}_{L/K}(\alpha) := tr\phi_\alpha$$

e **norma** di α il determinante dell'applicazione lineare

$$\mathrm{N}_{L/K}(\alpha) := \det \phi_a$$

Seguono dalla definizione alcune semplici proprietà:

1. $\mathrm{Tr}_{L/K}(\alpha), \mathrm{N}_{L/K}(\alpha) \in K$;
2. $\mathrm{Tr}_{L/K}(\cdot)$ è K-lineare: $\mathrm{Tr}(ax + by) = a\,\mathrm{Tr}(x) + b\,\mathrm{Tr}(y)$;
3. $\mathrm{N}_{L/K}(\cdot)$ è moltiplicativa: $\mathrm{N}(ab) = \mathrm{N}(a)\,\mathrm{N}(b)$;
4. $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(z) = \|z\|^2$.

Lemma 2.51. *Sia L/K un'estensione di grado n.*

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

Dimostrazione. Per la (1) basta notare che si ha $[\phi_\alpha] = \alpha I$. Per la (2), basta mostrare che μ_α coincide col polinomio caratteristico di ϕ_α: $\mu_\alpha = p_{\phi_\alpha}$. Questo risulta ovvio se si considera la base $(1, \ldots, \alpha^{n-1})$; la matrice che rappresenta ϕ_α risulta essere la matrice compagna di μ_α. □

Lemma 2.52. *Siano L/K finita e $\alpha \in L$ tale che $[L : K(\alpha)] = s$. Allora:*

1. $\mathrm{Tr}_{L/K}(\alpha) = s\,\mathrm{Tr}_{K(\alpha)/K}(\alpha)$;
2. $\mathrm{N}_{L/K}(\alpha) = (\mathrm{N}_{K(\alpha)/K}(\alpha))^s$.

Dimostrazione. Sia $(1, \beta_2, \ldots, \beta_s)$ una base di L su $K(\alpha)$. Allora la matrice che rappresenta ϕ_α rispetto alla base

$$(1, \alpha, \ldots, \alpha^{n-1}, \beta_2, \ldots, \beta_2\alpha^{n-1}, \ldots, \beta_s, \ldots, \beta_s\alpha^{n-1})$$

è diagonale a blocchi con blocchi tutti uguali alla matrice compagna del polinomio minimo di α, da cui la tesi. □

Teorema 2.53. *Sia L/K finita con $[L:K] = [L:K]_i[L:K]_s = q \cdot r$. Sia $\{\sigma_1, \dots, \sigma_r\} = \mathrm{Hom}_K(L, \overline{K})$. Allora per ogni $\alpha \in L$*

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

In particolare, se $q \neq 1$ (estensione non separabile), allora $\mathrm{Tr}_{L/K}(\alpha) = 0$.

Dimostrazione. Distinguiamo tre casi:

- Se $\alpha \in K$, segue dal fatto che α viene fissato da ogni immersione.
- Se $L = K(\alpha)$, sia $\mu_\alpha = x^n + c_1 x^{n-1} + ... + c_n$ il polinomio minimo di α. Sappiamo che $\mathrm{Tr}_{L/K}(\alpha) = -c_1$ e $\mathrm{N}_{L/K}(\alpha) = (-1)^n c_n$. D'altronde,

  $$\mu = \prod_{i=1}^{r} (x - \sigma_i(\alpha))^q = [x^r - \sum \sigma_i(\alpha) x^{r-1} + \cdots + (-1)^r \prod_{i=1}^{r} \sigma_i(\alpha)]^q$$

  da cui la tesi.
- Se $\alpha \in L$, poniamo $[L : K(\alpha)] = s$ e applichiamo il lemma precedente. Supponiamo $[L : K(\alpha)] = q_1 \cdot r_1$ e $[K(\alpha) : K] = q_2 \cdot r_2$ e riconduciamoci ai due casi precedenti. Sappiamo che la tesi è vera per α sulle estensioni $L/K(\alpha)$ e $K(\alpha)/K$. Sia $\mathrm{Hom}_K(K(\alpha), \overline{K}) = \{\tau_1, \dots, \tau_{r_1}\}$. Di conseguenza,

  $$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= [L : K(\alpha)] \cdot \mathrm{Tr}_{K(\alpha)/K}(\alpha) \\ &= q_1 \cdot r_1 \cdot q_2 \cdot \sum_{i=1}^{r_2} \tau_i(\alpha) \\ &= q \cdot \sum_{i=1}^{r_2} r_1 \tau_i(\alpha) \\ &\overset{(*)}{=} q \cdot \sum_{i=1}^{r} \sigma_i(\alpha) \end{aligned}$$

  dove $(*)$ è dovuto al fatto che per ogni τ_i ci sono r_1 estensioni σ_i tali che $\sigma_i(\alpha) = \tau_i(\alpha)$. Si ha un ragionamento analogo per $\mathrm{N}_{L/K}(\alpha)$.

□

Corollario 2.54. *Se L/K è normale e $\sigma \in \mathrm{Aut}(L)$,*

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L/K}(\sigma(\alpha)) \qquad \mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{L/K}(\sigma(\alpha))$$

Corollario 2.55. *Se $K \subset L \subset M$, allora*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} \qquad \mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$$

Corollario 2.56. *Sia L/K finita, $[L : K] = n$. Allora:*

1. *L/K è separabile se e solo se $\mathrm{Tr}_{L/K}$ è non banale (e dunque surgettiva).*
2. *Se L/K è separabile, il prodotto scalare $tr : (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ è non degenere e dunque $\phi : L \to L^\vee$ con $x \mapsto \mathrm{Tr}_{L/K}(x\cdot)$ è un isomorfismo.*

Dimostrazione.

1. $\Leftarrow$ Segue dal teorema.

   $\Rightarrow$ Se L/K è separabile si ha che $\mathrm{Tr}_{L/K} = \sigma_1 + \cdots + \sigma_n$ è somma di caratteri distinti e dunque per il teorema di indipendenza dei caratteri, sono linearmente indipendenti. Segue che $\mathrm{Tr}_{L/K}$ è non banale.

2. Il prodotto scalare è non degenere per il primo punto e quindi fornisce l'identificazione desiderata.

□

Corollario 2.57. *Sia L/K separabile. Sia $(x_1, \ldots, x_n)$ una K-base di L. Allora esiste $(y_1, \ldots, y_n)$ K-base di L (detta* **base duale***) tale che $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$.*

Dimostrazione. Dato che L è un K-spazio vettoriale di dimensione finita dotato di un prodotto scalare non degenere, fissata una base abbiamo due identificazioni con il duale. La prima, che chiamiamo ψ, è tale che $\psi(x_i)(x_j) = \delta_{ij}$. La seconda, che è quella indotta dal prodotto scalare, è la ϕ del corollario precedente. Basta allora considerare allora $y_i = \phi^{-1} \circ \psi(x_i)$. □

Esercizio 2.58. Sia L/K un'estensione finita e separabile, sia $(x_1, \ldots, x_n)$ una K-base di L e sia F una sottoestensione di L/K. Allora

$$F = K(\mathrm{Tr}_{L/F}(x_1), \ldots, \mathrm{Tr}_{L/F}(x_n))$$

Dimostrazione. Basta notare che, dato che l'estensione è separabile, l'applicazione $\mathrm{Tr}_{L/F} : L \to F$ è lineare e surgettiva e quindi l'immagine di una base di L genera F. □

Esercizio 2.59. Sia L/K separabile e finita di grado n, $L = K(\alpha)$. Siano $\mathcal{B} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ una base di L, f il polinomio minimo di α su K e

$$\frac{f}{x - \alpha} = \beta_{n-1} x^{n-1} + ... + \beta_1 x + \beta_0$$

Allora la base duale di $\mathcal{B}$ é

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

Dimostrazione. Preliminarmente, notiamo che, dette $\alpha_1, \ldots, \alpha_n$ le radici di f, il polinomio

$$x^r - \sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)}$$

è nullo, in quanto ha grado $\leq n-1$ e ha radici $\alpha_1, \ldots, \alpha_n$. Di conseguenza si ha

$$\mathrm{Tr}_{L/K}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\right) = x^r$$

dove con traccia di un polinomio intendiamo il polinomio a cui applichiamo la traccia a ogni coefficiente. D'altronde,

$$\begin{aligned}\mathrm{Tr}_{L/K}\left(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}\right) &= \mathrm{Tr}_{L/K}\left(\sum_{i=0}^{n-1}\frac{\beta_i x^i}{f'(\alpha)}\alpha^r\right) \\ &= \sum_{i=0}^{n-1} x^i \,\mathrm{Tr}_{L/K}\left(\frac{\beta_i \alpha^r}{f'(\alpha)}\right)\end{aligned}$$

Di conseguenza si ottiene

$$\mathrm{Tr}_{L/K}\left(\frac{\beta_i}{f'(\alpha)}\alpha^r\right) = \delta_{ir}$$

come voluto. □

Capitolo 3

Teoria di Kummer e sue applicazioni

3.1 Teoria delle estensioni cicliche

Iniziamo ora lo studio estensioni cicliche a partire dal *Teorema* 90 *di Hilbert*, proponendone due versioni: la prima è quella classica che utilizza strumenti a noi ora noti; l'altra è coomologica, di gusto più moderno ma utile per liberarci dalla condizione di ciclicità dell'estensione.

Teorema 3.1 (Teorema 90 di Hilbert, classico)**.** *Sia L/K estensione ciclica di grado n con* $\mathrm{Gal}(L/K) = G =< \sigma >$*. Allora:*

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

Dimostrazione.

1. $\Leftarrow$ Segue da $\mathrm{N}_{L/K}(\beta) = \mathrm{N}_{L/K}(\sigma(\beta))$.

   $\Rightarrow$ Sia $\alpha \in L^\times$ tale che $\mathrm{N}_{L/K(\alpha)} = 1$. Consideriamo la somma di caratteri

   $$\chi = 1 + \alpha\sigma + \alpha\sigma(\alpha)\sigma^2 + ... + \Big(\prod_{i=0}^{n-2} \sigma^i(\alpha)\Big)\sigma^{n-1}$$

   Per il teorema di indipendenza dei caratteri (2.49), $\chi \neq 0$, per cui esiste $\gamma \in L^\times$ tale che $\chi(\gamma) \neq 0$. Posto $\beta = \chi(\gamma)$, abbiamo

   $$\beta = \gamma + \alpha\sigma(\gamma) + ... + \prod_{i=0}^{n-2} \sigma^i(\alpha)\sigma^{n-1}(\gamma)$$

Calcoliamo $\sigma(\beta)$:

$$\sigma(\beta) = \sigma(\gamma) + \sigma(\alpha)\sigma^2(\gamma) + \cdots + \Big(\prod_{i=1}^{n-1} \sigma(\alpha)\Big)\gamma$$

Di conseguenza,

$$\alpha\sigma(\beta) = \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \Big(\prod_{i=0}^{n-1} \sigma(\alpha)\Big)\gamma$$

Ma $\prod_{i=0}^{n-1} \sigma^i(\alpha) = \mathrm{N}_{L/K}(\alpha) = 1$. Segue che $\alpha\sigma(\beta) = \beta$.

2. $\Leftarrow$ Segue da $\mathrm{Tr}_{L/K}(\beta) = \mathrm{Tr}_{L/K}(\sigma(\beta))$.

   $\Rightarrow$ Poiché L/K è separabile, esiste $\gamma \in L$ tale che $\mathrm{Tr}_{L/K}(\gamma) \neq 0$. Consideriamo l'elemento

$$\beta = \frac{1}{\mathrm{Tr}_{L/K}(\gamma)}(\alpha\sigma(\gamma) + \cdots + \Big(\sum_{i=0}^{n-2} \sigma^i(\alpha)\Big)\sigma^{n-1}(\gamma)\ )$$

   Allora in $\sigma(\beta)$ l'ultimo addendo è

$$(\sum_{i=1}^{n-1} \sigma^i(\alpha))\sigma^n(\gamma) = (\mathrm{Tr}_{L/K}(\alpha) - \alpha)\gamma \overset{\mathrm{Tr}_{L/K}(\alpha)=0}{=} -\alpha\gamma$$

   Segue che $\alpha = \beta - \sigma(\beta)$.

□

Prima di presentare la versione coomologica, abbiamo bisogno di qualche definizione.

Definizione 3.2. Siano G gruppo e A gruppo abeliano. A è un **G-modulo** se G agisce su A tramite $\phi\colon G \to \mathrm{Aut}(A)$ definita da

$$g \cdot a := \phi_g(a)$$

Definizione 3.3. Dati G gruppo e A gruppo abeliano, definisco:

- 1-**cocicli** (o **omomorfismi crociati**):

$$Z^1(G, A) \coloneqq \{f : G \to A \mid f(\sigma \circ \sigma') = \sigma f(\sigma') *_A f(\sigma)\}$$

- 1-**cobordi**:

$$B^1(G, A) \coloneqq \{f : G \to A \mid \exists a \in A,\ f(\sigma) = \sigma(a)^{-1} *_A a\ \forall \sigma \in G\ \}$$

- **primo gruppo di coomologia**:

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

É ben definito in quanto $B^1(G, A) \triangleleft Z^1(G, A)$.

Teorema 3.4 (Teorema 90 di Hilbert, coomologico)**.** *Sia L/K di Galois finita con $G = \mathrm{Gal}(L/K)$. Allora:*

1. *(moltiplicativo) $H^1(G, L^\times) = \{1\}$;*
2. *(additivo) $H^1(G, L) = \{0\}$.*

Dimostrazione.

1. (moltiplicativo) Dobbiamo mostrare che ogni 1-cociclo è un 1-cobordo. Sia $f : G \to L^\times \in Z^1(G, L^\times)$ un 1-cociclo; per definizione

$$f(\sigma \circ \sigma') = \sigma f(\sigma') \cdot f(\sigma)$$

Notiamo che $\sum_{\sigma' \in G} f(\sigma')\sigma'$ è una combinazione non banale di caratteri, dunque esiste $c \in L^\times$ tale che $b = \sum_{\sigma' \in G} f(\sigma')\sigma'(c) \neq 0$. Mostriamo che $f(\sigma) = \sigma(b)^{-1}b$, da cui seguirà che $f \in B^1(G, L^\times)$. Calcoliamo $\sigma(b)$:

$$\sigma(b) = \sum_{\sigma' \in G} \sigma(f(\sigma'))(\sigma \circ \sigma')(c)$$

Dato che $f \in Z^1(G, L^\times)$, $\sigma f(\sigma') = f(\sigma)^{-1} f(\sigma \circ \sigma')$, da cui

$$\begin{aligned} \sigma(b) &= f(\sigma)^{-1} \sum_{\sigma' \in G} f(\sigma \circ \sigma')(\sigma \circ \sigma')(c) \\ &= f(\sigma)^{-1} \sum_{\sigma' \in G} f(\sigma')\sigma'(c) \\ &= f(\sigma)^{-1} b \end{aligned}$$

ossia f è un 1-cobordo. Da $Z^1(G, L^\times) = B^1(G, L^\times)$ segue che

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

2. (additivo) Dobbiamo mostrare che ogni 1-cociclo è un 1-cobordo, ossia

$$f(\sigma \circ \sigma') = \sigma f(\sigma') + f(\sigma) \implies \exists a \in L \mid f(\sigma) = a - \sigma(a)$$

Sia $f : G \to L$ un 1-cociclo. Poiché L/K é separabile, esiste $c \in L$ tale che $\mathrm{Tr}_{L/K}(c) \neq 0$. Considero

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

e applico σ

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

Poiché f é 1-cociclo, $\sigma f(\sigma') = f(\sigma \circ \sigma') - f(\sigma)$, da cui

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

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

$$= b - \frac{1}{\mathrm{Tr}_{L/K}(c)} f(\sigma)\,\mathrm{Tr}_{L/K}(c) = b - f(\sigma)$$

Segue che $f(\sigma) = b - \sigma(b)$, ossia f é un 1-cobordo. Dunque si ha

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

□

Vediamo che la versione coomologica implica quella classica.

Proposizione 3.5. *Hilbert 90 coomologico* $\implies$ *Hilbert 90 classico.*

Dimostrazione. Sia L/K ciclica di grado n con gruppo di Galois $G =< \sigma >$. Sia $\alpha \in L^\times$ tale che $\mathrm{N}_{L/K}(\alpha) = 1$. Vogliamo trovare $\beta \in L^\times$ per cui $\alpha\sigma(\beta)^{-1} = \beta$. Consideriamo $f : G \to L^\times$ tale che

$$1 = \sigma^0 \mapsto 1 \quad , \quad \sigma^k \mapsto \prod_{i=0}^{k-1} \sigma^i(\alpha) \qquad \forall 1 \leq k \leq n-1$$

Si verifica che f é un 1-cociclo (si usa l'ipotesi $\mathrm{N}_{L/K}(\alpha) = 1$): dunque, per Hilbert 90 coomologico (3.4), f é un 1-cobordo, ossia esiste $\beta \in L^\times$ tale che $\alpha = f(\sigma) = \sigma(\beta)^{-1}\beta$ (cioé la tesi).
La dimostrazione della versione additiva é del tutto analoga.

□

L'Hilbert 90 ha due conseguenze molto importanti sulle estensioni cicliche:

Teorema 3.6 (Kummer)**.** *Sia K un campo tale che $\zeta_n \in K$ e* $\mathrm{char}\, K \nmid n$.

1. *Se L/K è un'estensione ciclica di grado n, allora esiste $\alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha = x^n - c \in K[x]$.*

2. *Se $L = K(\alpha)$ con α radice di $x^n - c$, allora L/K è un'estensione ciclica di grado $d \mid n$ e $\mu_\alpha = x^d - \alpha^d \in K[x]$.*

Dimostrazione.

1. Sia $G = \mathrm{Gal}(L/K) =< \sigma >$ con $\mathrm{ord}(\sigma) = n$. Sappiamo che $\mathrm{N}_{L/K}(\zeta_n^{-1}) = 1$. Per Hilbert 90 (3.1), esiste $\alpha \in L^\times$ tale che $\zeta_n^{-1}\sigma(\alpha) = \alpha$, ossia $\sigma(\alpha) = \zeta_n\alpha$; quindi $\sigma^k(\alpha) = \zeta_n^k\alpha$. Consideriamo l'orbita
$$\mathrm{orb}_G(\alpha) = \{\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha\}$$
Notiamo che $\sigma^i(\alpha) \neq \sigma^j(\alpha)$ per ogni $i \neq j$ in quanto $\mathrm{char}\, K \nmid n$ e $\zeta_n^i \neq \zeta_n^j$. Ne segue che $[K(\alpha) : K] = n$, dunque $L = K(\alpha)$. Inoltre,
$$\mu_\alpha = \prod_{i=0}^{n-1}(x - \zeta_n^i\alpha) = x^n - \alpha^n$$

2. Supponiamo $\alpha \neq 0$ e poniamo $f(x) = x^n - c$ (si ha $f(\alpha) = 0$). Allora gli zeri di f sono $\{\zeta_n^i\alpha\}_{i=0}^{n-1}$. Poiché $\zeta_n \in K \subset L$, si ha che gli zeri di μ_α sono contenuti in $L = K(\alpha)$, ossia L/K è normale. Inoltre, L/K è separabile in quanto lo è f (infatti, essendo $\mathrm{char}\, K \nmid n$, per $i \neq j$ $\zeta_n^i \neq \zeta_n^j$). Dunque L/K é di Galois; mostriamo che $G = \mathrm{Gal}(L/K)$ è ciclico. Consideriamo l'omomorfismo iniettivo
$$\begin{array}{ccc} G & \longrightarrow & < \zeta_n > \\ \sigma & \longmapsto & \zeta_n^{j_\sigma} = \frac{\sigma(\alpha)}{\alpha} \end{array}$$
G è allora ciclico di ordine $d \mid n$. Rimane solo da trovare il polinomio minimo di μ_α. Sia $G =< \sigma_0 >$: si ha $\sigma_0 \mapsto \zeta_n^{i_0} = \frac{\sigma_0(\alpha)}{\alpha}$ e $d = |G| = \mathrm{ord}\,\sigma_0 = \mathrm{ord}\,\zeta_n^{i_0}$. Allora $\sigma_0(\alpha^d) = \sigma_0(\alpha)^d = \zeta_n^{i_0 d}\alpha^d = \alpha^d$, per cui $\alpha^d \in K$. Dunque $\mu_\alpha \mid x^d - \alpha^d$ e per motivi di grado vale l'uguaglianza.

□

Teorema 3.7 (Artin-Schreier)**.** *Sia K un campo di* $\mathrm{char}\, K = p$.

1. *Se L/K è un'estensione ciclica di grado p, allora esiste $\alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha = x^p - x - c \in K[x]$;*

2. *Se $L = K(\alpha)$ con α radice di $x^p - x - c \in K[x]$, allora L/K è ciclica di grado 1 o p. In particolare,*
$$[L : K] = \begin{cases} 1 & \text{se } x^p - x - c \text{ si spezza completamente} \\ p & \text{se } x^p - x - c \text{ è irriducibile} \end{cases}$$

Dimostrazione.

1. Poiché $\mathrm{Tr}_{L/K}(-1) = p = 0$, per Hilbert 90 esiste $\alpha \in L$ tale che $-1 = \alpha - \sigma(\alpha)$, $\sigma(\alpha) = \alpha + 1$. Dunque $\sigma^i(\alpha) = \alpha + i$ e
$$\mathrm{orb}_G(\alpha) = \{\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + p - 1\}$$
Poiché $K(\alpha)/K$ è separabile, $[K(\alpha) : K] = p$ e $K(\alpha) = L$. Inoltre, $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, ossia $\alpha^p - \alpha \in \mathrm{Fix}(\sigma)$. Quindi $\alpha^p - \alpha = c \in K$ e $\mu_\alpha = x^p - x - c \in K[x]$.

2. Sia α radice di $f(x) = x^p - x - c \in K[x]$. Notiamo che, essendo in caratteristica p, $f(\alpha + i) = 0$ per ogni $0 \leq i \leq p-1$. Gli zeri di f sono $\{\alpha, \alpha+1, \ldots, \alpha+p-1\}$: segue che f è separabile, dunque lo è $L = K(\alpha)$. Inoltre, L/K è normale, quindi di Galois. Sia $[L:K] = d$: si ha $|\operatorname{orb}_G(\alpha)| = d$. Consideriamo

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

Dunque $d\alpha \in K$ e ho due casi: se $d = 0 \in K$, allora $p|d$ in $\mathbb{Z}$ e $[L:K] = p$; se $d \neq 0$, allora $\alpha \in K$ e $[L:K] = 1$.

□

Vediamo ora che è possibile dimostrare i teoremi di Kummer e Artin-Schreier senza ricorrere al Teorema 90 di Hilbert, ma usando solo strumenti di base di algebra lineare.

Proposizione 3.8 (Kummer, pto 1.)**.** *Sia L/K ciclica di grado n, con* $\operatorname{char} K \nmid n$ *e $\zeta_n \in K$. Allora esiste $\alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha = x^n - c$.*

Dimostrazione. Dobbiamo mostrare che esiste $\alpha \in L^\times$ tale che $\sigma(\alpha) = \zeta_n\alpha$ (dopodiché la dimostrazione prosegue come quella giá vista).
Sia $\operatorname{Gal}(L/K) =< \sigma >$: consideriamo σ come applicazione K-lineare. Poiché $\sigma^n = id$, il polinomio caratteristico di σ è $x^n - 1$ e quindi ζ_n è un autovalore per σ: ne segue che esiste $\alpha \in L^\times$ che é autovettore per σ relativo a ζ_n, ossia $\sigma(\alpha) = \zeta_n\alpha$. □

Proposizione 3.9 (Artin-Schreier, pto 1.)**.** *Sia* $\operatorname{char} K = p$ *e sia L/K ciclica di grado p. Allora esiste $\alpha \in L$ tale che $L = K(\alpha)$ e $\mu_\alpha = x^p - x - c \in K[x]$.*

Dimostrazione. Basta mostrare che esiste $\alpha \in L$ tale che $\sigma(\alpha) - 1 = \alpha$. Sia $\operatorname{Gal}(L/K) =< \sigma >$ con $\sigma^p = 1$: allora il polinomio caratteristico di σ come applicazione K-lineare é $x^p - 1$ e coincide col polinomio minimo di σ in quanto, essendo $\operatorname{char} K = p$, $x^p - 1 = (x-1)^p$ e $\{1, \sigma, \ldots, \sigma^{p-1}\}$ sono indipendenti (per l'indipendenza dei caratteri). Dalla teoria di Jordan, sappiamo che σ è simile a un blocco di Jordan. Chiamando $v_1, \ldots, v_p$ i vettori di una base di Jordan per σ, abbiamo che

$$\sigma(v_1) = v_1 \ , \ \sigma(v_k) = v_k + v_{k-1} \ \forall 2 \leq k \leq p$$

e quindi (poiché $v_1 \in K$ in quanto fissato da σ) si ha

$$\sigma\Big(\frac{v_2}{v_1}\Big) = \frac{\sigma(v_2)}{v_1} = \frac{v_2}{v_1} + 1$$

ossia per $\alpha = \frac{v_2}{v_1}$ si ha $\sigma(\alpha) = \alpha + 1$. □

Proponiamo ora un risultato di Artin che generalizza la relazione $\mathbb{C} = \mathbb{R}(i)$.

Teorema 3.10 (Teorema di Artin)**.** *Siano K un campo e sia $\overline{K}$ una sua chiusura algebrica con $i \in \overline{K}$ tale che $i^2 = -1$. Se $[\overline{K} : K] < \infty$, allora $\overline{K} = K(i)$. Inoltre, se $\overline{K}/K$ è non banale, allora* $\operatorname{char} K = 0$.

Dimostrazione. Osserviamo che $\overline{K}/K$ è normale. Inoltre $\overline{K}/K$ è separabile: se così non fosse, avremmo che la sua chiusura perfetta sarebbe un'estensione algebrica di grado infinito ed essendo algebrica sarebbe contenuta in $\overline{K}$. Dunque $\overline{K}/K$ è di Galois finita, e lo è anche $\overline{K}/K(i)$.
Supponiamo per assurdo che $K(i) \subsetneq \overline{K}$. Sia $G = \operatorname{Gal}(\overline{K}/K(i))$: per il teorema di Cauchy, dato l primo tale che $l \mid |G|$, esiste $H < G$ tale che $|H| = l$. Detto $L = \overline{K}^H$, abbiamo la torre di estensioni

$$\begin{array}{c} \overline{K} \\ {\scriptstyle l}\,| \\ L \\ | \\ K(i) \\ | \\ K \end{array}$$

Abbiamo due casi:

- Se $\operatorname{char} K = l$, per il teorema di Artin-Schreier (3.7) sull'estenione ciclica $\overline{K}/L$, esiste $a \in \overline{K}$ tale che $\overline{K} = L(a)$ e $\mu_a = x^l - x - c \in L[x]$. Consideriamo allora la mappa surgettiva

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

  È facile verificare che $\operatorname{Tr}_{\overline{K}/L} \circ \tau = \tau|_L \circ \operatorname{Tr}_{\overline{K}/L}$. Poiché $\operatorname{Tr}_{\overline{K}/L}$ e τ sono surgettive, lo è anche $\tau|_L$. Di conseguenza, esiste $\alpha \in L$ tale che $\alpha^l - \alpha - c = 0$; ma ciò è assurdo in quanto μ_a è irriducibile su L.

- Se $p = \operatorname{char} K \neq l$, sappiamo che $\overline{K}/L$ è ciclica di grado l. Inoltre, $\zeta_l \in L$: se così non fosse, avremmo $[L(\zeta_l) : L] = l - 1$ ma $[\overline{K} : L] = l$ e $l - 1 \nmid l$, da cui un assurdo. Per il teorema di Kummer (3.6) esiste $a \in \overline{K}$ tale che $\overline{K} = L(a)$ e $\mu_a = x^l - c \in L[x]$. Consideriamo $\alpha \in \overline{K}$ con $\alpha^l = a$: si ha

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

  Se l è un primo dispari, allora $\operatorname{N}_{\overline{K}/L}(\alpha)^l = c$ e quindi $\operatorname{N}_{\overline{K}/L}(\alpha)$ è radice di $x^l - c$: ciò è assurdo perché μ_a è irriducibile. Se invece $l = 2$, allora $\operatorname{N}_{\overline{K}/L}(\alpha)^2 = -c$ è un quadrato in L e, poiché $i \in L$, lo è anche c: ciò è assurdo perché μ_a è irriducibile.

Da questo segue che $\overline{K} = K(i)$, in quanto $[\overline{K} : K(i)]$ ha grado che non è divisibile per nessun primo.
Supponiamo ora che $[\overline{K} : K] = 2$ e vediamo che in questo caso -1 non è un quadrato in K. Osserviamo che poiché $K(i) = \overline{K}$, somma di quadrati in K è un quadrato in K. Infatti, se $a, b \in K$, considero $a + ib \in K(i)$ e so che esistono $x, y \in K$ tali che $a + ib = (x + iy)^2$, per cui $a^2 + b^2 = (x^2 + y^2)^2$ è un quadrato in K. Se per assurdo $\operatorname{char} K = p \neq 0$, avremmo $-1 = p - 1 = 1 + ... + 1$: ma -1 non è quadrato in K, mentre $p - 1$ lo è, e dunque deve valere $\operatorname{char} K = 0$. □

Esercizio 3.11. Sia $\alpha \in \overline{\mathbb{Q}} - \mathbb{Q}$.

1. Esiste un sottocampo massimale $E \subset \overline{\mathbb{Q}}$ che non contiene α.
2. Ogni estensione F/E finita è ciclica.
3. Se $\overline{\mathbb{Q}}/E$ è infinita, $\operatorname{Gal}(\overline{\mathbb{Q}}/E) = \mathbb{Z}_p$, per qualche p primo.

Dimostrazione.

1. Sia $\mathcal{F} = \{L \subset \overline{\mathbb{Q}} \mid \alpha \notin L\}$: é un insieme induttivo e ammette quindi un elemento massimale E per Zorn.
2. $\forall\ E \subsetneq F,\ E \subsetneq E(\alpha) \subset F$. Sia F/E di Galois finita e sia $G = \operatorname{Gal}(F/E)$. Sia $H \lneq G$ tale che $F^H = E(\alpha)$: allora H é sottogruppo massimo (ossia contiene *ogni* sottogruppo proprio) in quanto $E(\alpha) = F^H \subset F^{H'} \Rightarrow H' \subset H$. Allora $\forall\ x \in G - H, < x >= G$: segue che F/E é ciclica.
3. Sappiamo che ogni estensione finita F/E é ciclica e che $G = \operatorname{Gal}(F/E)$ ha un sottogruppo massimo: allora $G = \operatorname{Gal}(F/E) \cong \mathbb{Z}/p^n\mathbb{Z}$.
   Inoltre, $G_\alpha = \operatorname{Gal}(E(\alpha)/E)$ é ciclico e isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Inoltre, $\forall m < n$ esiste *al piú* un'estensione F/E di grado p^n (altrimenti si avrebbe $FF'/E(\alpha)$ non ciclica). Sappiamo che se $\overline{\mathbb{Q}}/E$ é finita e $\alpha = i$, allora $\operatorname{Gal}(\overline{\mathbb{Q}}/E) \cong \mathbb{Z}/2\mathbb{Z}$.
   Sia $\overline{\mathbb{Q}}/E$ infinita. Allora, al variare di F/E finita, si ha

   $$\operatorname{Gal}(\overline{\mathbb{Q}}/E) = \varprojlim \operatorname{Gal}(F/E)$$

   e, poiché ha grado infinito, per n abbastanza grande esiste F/E di grado p^n, per cui $\varprojlim \operatorname{Gal}(F/E) = \mathbb{Z}_p$, e dunque

   $$\operatorname{Gal}(\overline{\mathbb{Q}}/E) = \mathbb{Z}_p$$

□

3.2 Teorema della base normale

Sia A un anello commutativo con unità e sia G un gruppo. Consideriamo l'insieme

$$A[G] := \{\sum_{g\in G} a_g g \mid a_g \in A \text{ quasi tutti nulli}\}$$

munito delle operazioni

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

È facile dimostrare che $A[G]$ munito di queste operazioni è un anello, detto **anello di gruppo**. Notiamo che $\mathbb{1}_{A[G]} = \mathbb{1}_A \mathbb{1}_G$.

Possiamo vedere $A[G]$ come A-modulo libero generato da G. Inoltre notiamo che dire che M é un $A[G]$-modulo equivale a dire che M é un A-modulo e un G-modulo (3.2).

Esempio.

- Un gruppo abeliano M su cui è definita un'azione di un gruppo G è uno $\mathbb{Z}[G]$-modulo.
- Sia L/K un'estensione di Galois: allora $G = \mathrm{Gal}(L/K)$ agisce su L. L è un K-modulo su cui agisce G, dunque è un $K[G]$-modulo.

Definizione 3.12. Sia L/K finita e separabile. Sia $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Definiamo

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) \coloneqq (\det(\sigma_i(\alpha_j))_{i,j})^2$$

Osserviamo che, data $L = K(\alpha)$ di Galois di grado n con $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$, allora $(1, \alpha, \dots, \alpha^{n-1})$ è una K-base di L: si ha

$$\mathrm{disc}(1, \alpha, \dots, \alpha^{n-1}) = (\det(\sigma_i(\alpha^j)))^2 = \mathrm{disc}(\mu_\alpha)$$

Proposizione 3.13. *Sia L/K finita e separabile. Consideriamo le immersioni $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Allora $(\alpha_1, \dots, \alpha_n)$ è una K-base di L se e solo se*

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = (\det(\sigma_i(\alpha_j))_{i,j})^2 \neq 0$$

Dimostrazione. Notiamo che $\mathrm{disc}(\alpha_1, \dots, \alpha_n) = 0$ se e solo se

$$\det \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix} = 0$$

Il determinante è nullo se e solo se esiste una combinazione lineare delle colonne, ossia se esistono $c_1, \dots, c_n \in K$ non tutti nulli tali che

$$\sum_{i=1}^{n} c_i \begin{pmatrix} \sigma_1(\alpha_i) \\ \vdots \\ \sigma_n(\alpha_i) \end{pmatrix} = 0$$

Osservando la prima componente della relazione, si ha $\sum c_i \sigma_1(\alpha_i) = 0$, ossia $\sigma_1(\sum c_i \alpha_i) = 0$; per iniettività di σ_1, si ha $\sum c_i \alpha_i = 0$, cioè $\alpha_1, \dots, \alpha_n$ sono linearmente dipendenti. □

Lemma 3.14. *Sia K infinito e $S \subset K$ insieme infinito. Allora per ogni $f \in K[x_1, \dots, x_n]$ non nullo esistono $s_1, \dots, s_n \in S$ tali che $f(s_1, \dots, s_n) \neq 0$.*

Dimostrazione. Ragioniamo per induzione su n:

- $n = 1$: dato $f \in K[x] - \{0\}$ di grado n, sappiamo che ha al piú n radici, dunque poiché S é infinito vale la tesi.
- $n - 1 \Rightarrow n$: sia $f \in K[x_1 \dots x_n] - \{0\}$. Posso supporre che in f compaiano tutte le variabili, altrimenti sono giá nell'ipotesi induttiva. Prendo $s_n \in S$ tale che $f(x_1 \dots x_{n-1}, s_n) \not\equiv 0$: esiste poiché mi estendo a $K(x_1 \dots x_{n-1})[x_n]$ e mi riduco al passo base. Pongo $f(x_1 \dots x_{n-1}, s_n) = \tilde{f}(x_1 \dots x_{n-1}) \in K[x_1 \dots x_{n-1}] - \{0\}$: per ipotesi induttiva esistono $s_1 \dots s_{n-1} \in S$ tali che $0 \neq \tilde{f}(s_1 \dots s_{n-1}) = f(s_1 \dots s_{n-1}, s_n)$, cioé la tesi.

□

Proposizione 3.15. *Sia K infinito e sia L/K di Galois con gruppo di Galois $G = \{\sigma_1, \dots, \sigma_n\}$. Allora per ogni $f \in L[x_1, \dots, x_n]$ 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. Dalla proposizione 3.13, so che $A = (\sigma_i(\alpha_j))_{i,j}$ è invertibile, ossia $\det A \neq 0$. Consideriamo

$$\phi\colon \quad L[x_1, \dots x_n] \quad \longrightarrow \quad L[y_1, \dots, y_n], \quad x_i \longmapsto \textstyle\sum_{j=1}^{n} \sigma_i(\alpha_j) y_j$$

Dato che A è invertibile, lo è anche ϕ: dunque $g(y_1, \dots, y_n) = 0$ se e solo se $f(x_1, \dots, x_n) = 0$. Consideriamo $g \neq 0$: per il lemma precedente (K è infinito), esistono $s_1, \dots, s_n \in K$ tali che $g(s_1, \dots s_n) \neq 0$, ossia

$$\begin{aligned} 0 \neq g(s_1, \dots s_n) &= f(\sum_j \sigma_1(\alpha_j) s_j, \dots, \sum_j \sigma_n(\alpha_j) s_j) \\ &= f(\sigma_1(\sum_j \alpha_j s_j), \dots, \sigma_n(\sum_j \alpha_j s_j)) \end{aligned}$$

da cui la tesi. □

Osservazione. Si osservi che se K fosse finito, la proposizione #2 sarebbe falsa: posti $K = \mathbb{F}_q$ e $L = \mathbb{F}_{q^n}$, vale sempre $(id)^{q^n} - id \equiv 0$.

Lemma 3.16. *Sia V uno spazio vettoriale di dimensione n su un campo K. Sia $\phi \in End(V)$ tale che il polinomio caratteristico p_ϕ coincide con μ_ϕ. Allora esiste $v \in V$ tale che $V = Span(v, \phi(v), \dots, \phi^{n-1}(v))$.*

Dimostrazione. Notiamo che V può essere munito di una struttura di $K[x]$-modulo in maniera naturale, ponendo

$$x \cdot v = \phi(v)$$

Dato che $K[x]$ è un PID, possiamo allora decomporre V tramite la forma normale di Smith come

$$V \simeq \bigoplus_{i=1}^{r} K[x]/J_i$$

con la condizione $J_i \supseteq J_{i+1}$. Notiamo che

$$\mathrm{Ann}(V) = \bigcap_{i=1}^{r} J_i = (\mu_\phi)$$

Infatti, $\mu_\phi \in \mathrm{Ann}(V)$, da cui un contenimento. Se non valesse l'uguaglianza, esisterebbe $f \in \mathrm{Ann}(V) \setminus (\mu_\phi)$. Allora $(f, \mu_\phi) = s$, $s \mid \mu_\phi$ e $s(\phi) = 0$, da cui un assurdo per la minimalità di μ_ϕ. Di conseguenza, dato che gli ideali sono in catena, si ha $J_r = (\mu_\phi)$. Dato che $p_\phi = \mu_\phi$, $\dim_K K[x]/J_r = n = \dim_K V$ e dunque vale $r = 1$, ossia

$$V \simeq K[x]/(\mu_\phi)$$

Dunque, V ammette una base ciclica come K-spazio vettoriale, corrispondente a $(1, x, x^2, \dots, x^{n-1})$. □

Teorema 3.17 (Teorema della base normale)**.** *Sia L/K di Galois finita con gruppo di Galois $G = \mathrm{Gal}(L/K)$. Allora esiste $\alpha \in L$ tale che*

$$L = K[G]\alpha$$

ossia L é un $K[G]$-modulo ciclico generato da α.

Dimostrazione. Osserviamo che la tesi equivale a dire che esiste $\alpha \in L$ tale che $\{\sigma(\alpha)\}_{\sigma \in G}$ è una K-base di L. Nel caso K sia un campo finito, siano $|K| = q$, $[L : K] = n$ e $\mathrm{Gal}(L/K) = G = \langle \phi \rangle$ con $\phi : x \mapsto x^q$ il Frobenius. Consideriamo ϕ come mappa K-lineare e poniamo p_ϕ il suo polinomio caratteristico e q_ϕ il suo polinomio minimo: allora $p_\phi = x^n - 1$ coincide con q_ϕ per l'indipendenza dei caratteri. La tesi segue in questo caso dal lemma precedente.

Se invece K è infinito, cerchiamo $\alpha \in L$ tale che $(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$ sia una K-base di L. Per la proposizione 3.13, essa è una base se e solo se $\mathrm{disc}(\sigma_1(\alpha), \dots . \sigma_n(\alpha)) \neq 0$. Studiamo dunque $\det(\sigma_i(\sigma_j(\alpha)))_{i,j}$.
Notiamo che $\sigma_i \circ \sigma_j = \sigma_k$. Consideriamo

$$\varphi \colon \{1 \dots n\}^2 \longrightarrow \{1 \dots n\}$$

definita da $(i,j) \mapsto k$ con k tale che $\sigma_i \circ \sigma_j = \sigma_k$. Per la legge di cancellazione $\varphi(i, \cdot)$ e $\varphi(\cdot, j)$ sono iniettive. Sia dunque la matrice

$$X = (x_{\varphi(i,j)})_{i,j}$$

$\varphi(i, \cdot)$ iniettiva $\Rightarrow$ in ogni colonna compaiono una e una sola volta tutte le σ_i; $\varphi(\cdot, j)$ iniettiva $\Rightarrow$ in ogni riga compaiono una e una sola volta tutte le σ_i.
$\det X$ é un polinomio $d(x_1 \dots x_n)$. Dico che $d(x_1 \dots x_n) \neq 0$: infatti, se si sostituisce $(1, 0 \dots 0)$, si ha il determinante della matrice le cui colonne sono i vettori della base canonica permutati, ossia ± 1; segue che $d(x_1 \dots x_n) \neq 0$. Allora, per la proposizione 3.15, esiste $\alpha \in L$ tale che

$$d(\sigma_1(\alpha) \dots \sigma_n(\alpha)) \neq 0$$

ma $0 \neq d(\sigma_1(\alpha) \dots \sigma_n(\alpha)) = \det(\sigma_i(\sigma_j(\alpha)))_{i,j} = \det(\sigma_{\varphi(i,j)}(\alpha))_{i,j}$. Dalla proposizione 3.13 segue la tesi.

□

3.3 Risolubilitá di gruppi ed estensioni

Definizione 3.18. Sia G un gruppo. Una **serie normale** per G è una catena

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

tale che $G_i \triangleleft G_{i-1}$. Un gruppo G si dice **risolubile** se ammette una serie normale a quozienti abeliani, ossia

$$G_i \diagup G_{i+1}$$

è abeliano per ogni i.

Esempio.

- Ogni gruppo abeliano è risolubile.
- Ogni p-gruppo finito (di cardinalità p^n) è risolubile: infatti per Sylow esiste un sottogruppo di cardinalità p^{n-1} che é normale in quanto di indice p (il piú piccolo primo che divide l'ordine del gruppo) e il quoziente è necessariamente abeliano.

- $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$ è risolubile.

Osservazione. Se G è risolubile e finito, per il teorema di struttura possiamo raffinare la catena e ottenere che ogni quoziente abbia cardinalità un primo p e quindi sia ciclico. Per questo, basta sfruttare la corrispondenza e ricordare che questa preserva la normalità.

Definizione 3.19. Dato G gruppo, definiamo **derivato** di G il sottogruppo

$$G' = [G, G] = DG =< \{[g, h] = ghg^{-1}h^{-1} \mid g, h \in G\} >$$

Valgono le seguenti:

Proposizione 3.20.

- *G é abeliano se e solo se $G' = \{e\}$;*
- *Se $N \lhd G$, allora G/N è abeliano se e solo se $G' \subseteq N$.*

Definizione 3.21. Definiamo ricorsivamente

$$D^0G = G \ , \quad D^1G = [G, G] \ , \quad D^{i+1}G = [D^iG, D^iG]$$

La catena dei derivati è una catena a quozienti abeliani ($D^iG \lhd D^{i-1}G$). Vediamo ora un test di risolubilitá.

Proposizione 3.22. *G è risolubile $\iff \exists\, n \in \mathbb{N}$ tale che $D^nG = \{e\}$.*

Dimostrazione. Supponiamo che G sia risolubile e consideriamo una serie normale

$$G = G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$$

Procediamo per induzione. G/G_1 è abeliano e dunque $DG \subseteq G_1$. Per il passo induttivo, notiamo che G_i/G_{i+1} è abeliano e dunque

$$G_{i+1} \supseteq DG_i \supseteq D^{i+1}G$$

dove $DG_i \supseteq D^{i+1}G$ per ipotesi induttiva. L'altra freccia é ovvia.

□

Proposizione 3.23.

1. *Se G é risolubile, ogni suo sottogruppo $H < G$ è risolubile.*
2. *Dato $H \lhd G$, G è risolubile se e solo se H e G/H sono risolubili.*

Dimostrazione.

1. Dato che esiste $n \in \mathbb{N}$ tale che $D^nG = \{e\}$, si ha $D^nH \subseteq D^nG = \{e\}$.

2. Consideriamo la proiezione $\pi\colon G \to G/H$; questa commuta con il derivato perché $[\pi(g), \pi(h)] = \pi[g, h]$. Di conseguenza $D\pi(G) = \pi DG$, da cui il quoziente è risolubile.
   Viceversa, supponiamo che H e G/H siano risolubili. Sappiamo che $D^m H = \{e\}$ e $D^n(G/H) = \{e\}$. Dunque $D^n \pi G = \{e\}$ e dunque $D^n G \subseteq H$. Ma allora $D^m D^n G \subseteq D^m H = \{e\}$ e dunque il gruppo è risolubile.

□

Corollario 3.24. *Siano $G_1, \ldots, G_n$ gruppi. Allora $\prod G_i$ è risolubile se e solo se G_i è risolubile per ogni i.*

Definizione 3.25. Un'estensione finita L/K è **risolubile** se esiste una sovraestensione E/L tale che E/K è di Galois e $\mathrm{Gal}(E/K)$ è un gruppo risolubile.

Segue dalla definizione che:

- Se L/K è risolubile e F è un'estensione intermedia, allora F/K è risolubile;
- L/K risolubile $\implies$ L/K separabile, in quanto sottoestensione di un'estensione di Galois;
- Detta $\tilde{L}$ la chiusura normale di L, L/K é risolubile se e solo se $\mathrm{Gal}(\tilde{L}/K)$ è risolubile.

Proprietà delle estensioni risolubili La proprietà dello shift è rispettata, ossia se L/K risolubile allora LF/F è risolubile.

Dimostrazione. Sia $\tilde{L}$ la chiusura normale di L; basta mostrare che $\tilde{L}F/F$ sia risolubile. Possiamo supporre che L/K sia di Galois con $\mathrm{Gal}(L/K)$ risolubile. Dunque LF/F è di Galois e $\mathrm{Gal}(LF/F) < \mathrm{Gal}(L/H)$ e dunque è risolubile. □

La proprietà delle torri è rispettata, ossia

$$M/K \text{ è risolubile se e solo se } M/L \text{ e } L/K \text{ sono risolubili.}$$

Dimostrazione. Supponiamo prima che M/K sia risolubile. Possiamo supporre che M sia di Galois. Dunque L/K è risolubile e lo stesso vale per M/L perché $\mathrm{Gal}(M/L) < \mathrm{Gal}(M/K)$. Viceversa, supponiamo che le sottoestensioni siano risolubili. Utilizzando la proprietà dello shift, possiamo supporre che M, L siano normali su K. Mostriamo che $\mathrm{Gal}(M/K)$ è risolubile. Consideriamo la successione esatta

$$0 \to \mathrm{Gal}\left(M/L\right) \longrightarrow \mathrm{Gal}\left(M/K\right) \longrightarrow \mathrm{Gal}\left(L/K\right) \to 0$$

Dato che il primo e l'ultimo termine della successione sono risolubili, lo è anche quello centrale, da cui la tesi. □

La proprietà del composto segue di conseguenza.

Definizione 3.26. Un'estensione finita L/K si dice **risolubile per radicali** se esiste un sovracampo E e una catena

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

tale che $E_i = E_{i-1}(\alpha)$, dove $\alpha \in E_i$ è una delle seguenti

- una radice dell'unità;
- una radice del polinomio $x^n - a$ dove $\mathrm{char}(K) \nmid n$;
- una radice del polinomio $x^p - x - c$ e $\mathrm{char}(K) = p$.

Proprietà delle estensioni risolubili per radicali La proprietà dello shift è rispettata, ossia se L/K è risolubile per radicali allora LF/F è risolubile per radicali.

Dimostrazione. Sappiamo che esiste

$$K = E_0 \subseteq \cdots \subseteq E_n = E$$

e dunque otteniamo

$$F = FE_0 \subseteq \cdots \subseteq FE_n = FE$$

e dunque otteniamo la catena richiesta. □

Anche la proprietà delle torri è rispettata, ossia M/K è risolubile se e solo se lo sono L/K e M/L.

Dimostrazione. Se M/K è risolubile, allora sicuramente lo sono M/L e L/K. Viceversa, sappiamo che L/K è risolubile per radicali e dunque, per un certo sovracampo L', abbiamo

$$K = L_0 \subseteq \cdots \subseteq L'$$

Considerato il campo $L'M$, basta prolungare la catena di L' con una di M/L traslata. □

Teorema 3.27. *Sia L/K un'estensione finita. Allora L/K è risolubile se e solo se è risolubile per radicali.*

Dimostrazione. Supponiamo dapprima che L/K sia risolubile. Possiamo supporre che L/K sia di Galois. Sia

$$m = \prod_{\substack{p|[L:K] \\ p \neq \text{char } K}} p$$

Consideriamo allora $F = K(\zeta_m)$. Dato che F/L è risolubile per radicali e L/K è risolubile, basta mostrare che LF/F è risolubile per radicali. Sappiamo che LF/F è risolubile e di Galois, e dunque, considerata una serie normale a quozienti ciclici di ordine primo, possiamo ottenere per corrispondenza una catena di sottocampi. Quindi

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = LF$$

Ogni estensione F_i/F_{i-1} è di Galois ciclica di ordine primo p_i. Sappiamo che $p_i \mid m$ e dunque in F ci sono le radici p_i-esime dell'unità. Per i teoremi di Kummer e di Artin-Schreier otteniamo allora la tesi.

Mostriamo ora l'altra implicazione. Supponiamo che L/K sia risolubile per radicali.

$$K = E_0 \subseteq \cdots \subseteq E_n = E$$

Possiamo supporre che $E = L$. Basta mostrare che E_{i+1}/E_i è risolubile; per la proprietà delle torri otteniamo la tesi. Supponiamo allora $E_{i+1} = E_i(\alpha)$; vediamo i casi:

- Se α è una radice dell'unità, l'estensione è abeliana e dunque otteniamo la tesi.
- Se α è una radice di $x^p - x - a$ allora l'estensione è ciclica e otteniamo la tesi.
- Se α è una radice di $x^n - a$, consideriamo la catena

  $$E_i \to E_i(\zeta_n) \to E_{i+1}(\zeta_n)$$

  Basta mostrare che la seconda estensione è risolubile, ma questo è vero per il teorema di Kummer in quanto questa è ciclica.

□

Corollario 3.28. *L'equazione generale di grado n è risolubile per radicali se e solo se $n \leq 4$.*

Dimostrazione. Sappiamo che l'equazione generale di grado n ha gruppo di Galois isomorfo a $\mathcal{S}_n$. Inoltre, $\mathcal{S}_n$ è risolubile se e solo se $n \leq 4$: infatti per $n \geq 5$ $\mathcal{A}_n$ é semplice e

$$[\mathcal{S}_n, \mathcal{S}_n] = [\mathcal{A}_n, \mathcal{A}_n] = \mathcal{A}_n$$

e quindi, per il test 3.22, $\mathcal{S}_n$ non é risolubile; mentre per $n \leq 4$ si hanno le serie formali

$$\{e\} \subset \mathcal{A}_3 \subset \mathcal{S}_3$$
$$\{e\} \subset V_4 \subset \mathcal{A}_4 \subset \mathcal{S}_4$$

e si dimostra che sono a quozienti abeliani.

□

Definizione 3.29. Dati $a, b \in \mathbb{F}_p - \{0\}$, definiamo **sostituzione lineare** la mappa

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

e **sottogruppo lineare** il sottogruppo

$$F_p = \{\sigma_{a,b}\} < \mathcal{S}(\mathbb{F}_p)$$

Definizione 3.30. Un gruppo $G < \mathcal{S}_p$ si dice **lineare** se esiste una bigezione $\phi\colon \{1, \ldots, p\} \longrightarrow \mathbb{F}_p$ tale che $G \hookrightarrow F_p$.

I sottogruppi lineari sono legati alla risolubilità. Prima di vedere tale relazione, dato $\pi \in \mathcal{S}_p$ un p-ciclo, vediamo chi è il suo normalizzatore $N_{\mathcal{S}_p}(\pi)$. Sappiamo che, identificando in $\mathcal{S}_p$ π con $\langle\pi\rangle$, vale

$$|N_{\mathcal{S}_p}(\pi)| = |Z_{\mathcal{S}_p}(\pi)| \cdot |\operatorname{Aut}(\pi)| = p(p-1)$$

Mostriamo che $N(\pi) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$. Ovviamente $\langle\pi\rangle \lhd N_{\mathcal{S}_p}(\pi)$. Notiamo che

$$|\operatorname{orb}_{N(\pi)}(1)| \cdot |Stab_{N(\pi)}(1)| = |N_{\mathcal{S}_p}(\pi)|$$

e, poiché π è un p-ciclo, si ha $|Stab_{N(\pi)}(1)| = p-1$. Inoltre si ha $\langle\pi\rangle \cap Stab_{N(\pi)}(1) = \{e\}$ e quindi $N_{\mathcal{S}_p}(\pi) \simeq < \pi > \rtimes Stab_{N(\pi)}(1)$. Mostriamo che $Stab_{N(\pi)}(1)$ è ciclico: possiamo costruire la mappa

$$\begin{array}{ccc} Stab_{N(\pi)}(1) & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \sigma & \longmapsto & r \end{array}$$

dove r è tale che $\sigma\pi\sigma^{-1} = \pi^r$. Questa mappa è un omomorfismo iniettivo e per cardinalità si ha un isomorfismo. Dunque $N(\pi) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.

Proposizione 3.31. *Sia π un p-ciclo in $\mathcal{S}_p$. Allora $N_{\mathcal{S}_p}(\pi) \simeq F_p$.*

Dimostrazione. Sappiamo che $|N_{\mathcal{S}_p}(\pi)| = p(p-1)$ e dalla definizione di F_p si ha $|F_p| = p(p-1)$. Considerando la bigezione $\{1 \ldots p\} \to \mathbb{F}_p$ definita da $i \mapsto \bar{i}$, si ha che π corrisponde a $\sigma_{1,1}$. Allora

$$< \pi > = < \sigma_{1,1} > = < \sigma_{1,b} > \lhd F_p$$

quindi $F_p \subset N_{\mathcal{S}_p}(\pi)$ e per questione di cardinalità coincidono. □

Proposizione 3.32. *Sia $\sigma \in F_p$. Se σ ha almeno due punti fissi, allora $\sigma = id$.*

Proposizione 3.33. *Sia $G < \mathcal{S}_p$ che agisce transitivamente su $\{1, \dots, p\}$. Sono equivalenti:*

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

Dimostrazione.

(1) $\Rightarrow$ (2) Segue dal fatto che $G < N_{S_p}(\pi) \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$, che è risolubile.

(2) $\Rightarrow$ (1) Osserviamo che se G agisce transitivamente su $\{1, \dots, p\}$, allora $p \mid |G|$ e dunque G contiene un p-ciclo π. Inoltre, se G è risolubile e agisce transitivamente su $\{1, \dots, p\}$, allora $< \pi >$ è l'unico sottogruppo di ordine p normale in G. Infatti, per risolubilitá G ammette una serie normale a quozienti ciclici di ordine primo

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

e sia $p_i = |G_i/G_{i+1}|$.
Mostriamo che G_i agisce transitivamente su $\{1, \dots, p\}$ per ogni $i \leq n-1$: per induzione

- il passo base coincide con l'ipotesi;
- supponiamo ora che G_i agisce transitivamente su $\{1, \dots, p\}$ e mostriamo che lo stesso vale per G_{i+1}: date $B_1, \dots, B_r$ le orbite dell'azione, sappiamo che

$$p = \sum_{j=1}^{r} |B_j|$$

ma vale che

$$|B_j| = |orb(x_j)| = \frac{|G_i|}{|Stab_{G_i}(x_j)|}$$

Poiché G_{i-1} agisce transitivamente su $\{1, \dots, p\}$, fissati x, y, sappiamo che esiste $g \in G_{i-1}$ tale che $g(x) = y$. Allora

$$Stab_{G_i}(x) = gStab_{gG_ig^{-1}}(y)g^{-1}$$

e, dato che $G_i \triangleleft G_{i-1}$, $G_i = gG_ig^{-1}$ e

$$|Stab_{G_i}(x)| = |Stab_{G_i}(y)|$$

Di conseguenza, tutte le orbite hanno la stessa cardinalità d, da cui $p = rd$, dunque $d = 1$ oppure $d = p$. Ma almeno un'orbita è non banale (altrimenti $G_i = \{e\}$), e dunque tutte le orbite sono non banali. Dunque $d = p$ e $r = 1$, cioé l'azione è transitiva.

Abbiamo ottenuto che $p \mid |G_i|$ per ogni i: in particolare, $p \mid [G_{n-1} : G_n] = |G_{n-1}| = p_{n-1}$ e quindi $G_{n-1} =< \pi >$ è generato da un p-ciclo. Vediamo che questo é l'unico. Sappiamo che $p^2 \nmid |G|$, perché $G \subseteq \mathcal{S}_p$. Mostriamo che se $H < G$ di ordine p, si ha $H < G_i$ per ogni $i \leq n-1$ per induzione. Il passo base é vero per ipotesi; supponiamo $H < G_i$ e consideriamo

$$H =< x > \hookrightarrow G_i \to {}^{G_i}\!/_{G_{i+1}}$$

che è nulla in quanto $p \nmid |G_i/G_{i+1}|$ ($p \mid\mid |G|$). Allora $H < G_{n-1}$ e per cardinalitá si ha l'uguaglianza.
Dunque $< \pi >$ é l'unico sottogruppo normale in G di ordine p. Ció conclude in quanto $< \pi > \triangleleft G \Rightarrow G \subset N_{\mathcal{S}_p}(\pi)$, ossia G é lineare.

□

Applichiamo quanto visto ai gruppi di Galois.

Proposizione 3.34. *Sia $f \in K[x]$ irriducibile e separabile di grado p. Sia $L = \mathrm{cds}_K(f)$ e $G = \mathrm{Gal}(F/K)$. Se G è risolubile, allora $L = K(\alpha, \beta)$, dove α, β sono due radici qualsiasi di f.*

Dimostrazione. Chiaramente $K \subseteq K(\alpha, \beta) \subseteq L$. In particolare, per la corrispondenza di Galois esiste $H < G$ tale che $L^H = K(\alpha, \beta)$. Mostriamo che $H = \{e\}$. Sappiamo per la proposizione precedente che G è lineare; inoltre, per ogni $\sigma \in H$ si ha $\sigma(\alpha) = \alpha$ e $\sigma(\beta) = \beta$, da cui σ è lineare con 2 punti fissi e dunque $\sigma = id$. □

Corollario 3.35. *Se f irriducibile e separabile di grado p su $\mathbb{Q}$ ha almeno due radici reali e una non reale, allora G non è risolubile.*

Risolvente Sia $f \in \mathbb{Z}[x]$ e siano $\alpha_1, \ldots, \alpha_n$ le sue radici. Sia L il campo di spezzamento e sia $G = \mathrm{Gal}(L/\mathbb{Q})$. Dato $\gamma \in L$, $\gamma = p(\alpha_1, \ldots, \alpha_n)$, sia

$$R_{\mathcal{S}_n}(f, \gamma) = \prod_{\sigma \in \mathcal{S}_n} (x - \sigma L(\alpha))$$

Da questo polinomio, si deduce il gruppo di Galois in base all'azione del gruppo su $L(\alpha)$.

Gruppi di Galois su $\mathbb{Q}$ Sia $f \in M[x]$ un polinomio monico separabile di grado n e sia K il suo campo di spezzamento su M. Dette $\alpha_1, \ldots, \alpha_n$ le radici di f, $K = M(\alpha_1, \ldots, \alpha_n)$ e sia G il gruppo $\mathrm{Gal}(K/M)$ Dunque $G < \mathcal{S}_n$.

Proposizione 3.36. *Se $B_1, \ldots, B_r$ sono le orbite di $\{\alpha_1, \ldots, \alpha_n\}$ sotto l'azione di G, allora su M*

$$f(x) = \prod f_i(x)$$

con $f_i = \prod_{\alpha_j \in B_i} (x - \alpha_j)$.

Osserviamo che se G è ciclico, $G =< \sigma >$, le orbite coincidono con i cicli della permutazione. Dunque se $f = f_1, \ldots, f_r$ con $\deg f_i = d_i$, allora σ è di tipo $d_1 + \cdots + d_r$.

Teorema 3.37. *Sia A un UFD e sia K il suo campo dei quozienti. Sia $f \in A[x]$ monico e sia $\mathfrak{p} \subseteq A$ un ideale primo. Sia $\overline{f} \in A/\mathfrak{p}[x]$ e supponiamo che $f, \overline{f}$ non abbiano radici multiple. Se $G = \mathrm{Gal}(F/K)$ e $G' = \mathrm{Gal}(F'/K')$ (quelli di $\overline{f}$), allora $G' < G$ come sottogruppi di $\mathcal{S}\{\alpha_1, \ldots, \alpha_n\}$.*

Esempio. Sia $f(x) = x^5 - x - 1$. Allora

$$x^5 - x - 1 \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod 2$$

Invece è irriducibile modulo 5 per Artin-Schreier, in quanto non si spezza completamente in $\mathbb{F}_5[x]$. Di conseguenza

$$\mathrm{Gal}(f/\mathbb{F}_5) =< 5\text{-ciclo} > \quad \mathrm{Gal}(f/\mathbb{F}_2) =< 2 + 3\text{-ciclo} >$$

e dunque $\mathrm{Gal}(f/\mathbb{Q}) \simeq \mathcal{S}_5$ (perché $\mathrm{Gal}(f/\mathbb{Q})$ contiene un $2 + 3$-ciclo e un 5-ciclo).

3.4 Cenni di coomologia di gruppi

Definizione 3.38. Una successione di A-moduli

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

si dice **esatta** (corta) se

- f è iniettiva;
- g è surgettiva;
- $\mathrm{Im}\, f = \mathrm{Ker}\, g$.

Piú in generale, una successione di A-moduli $M \xrightarrow{f} N \xrightarrow{g} P$ si dice *esatta in N* se $\mathrm{Im}\, f = \mathrm{Ker}\, g$.
Si noti che $\mathrm{Im}\, f = \mathrm{Ker}\, g \implies g \circ f = 0$, ma il viceversa in generale é falso.
Riprendiamo la definizione di modulo su un gruppo.

Definizione 3.39. Siano A un anello commutativo con unitá, M un A-modulo e G un gruppo. Diciamo che M è **G-modulo** se é definita l'azione di G su M

$$G \longrightarrow \mathrm{Aut}(M)$$

(o equivalentemente, se M é un $A[G]$-modulo).

Ricordiamo che data L/K di Galois e $G = \mathrm{Gal}(L/K)$, allora L è $K[G]$-modulo ed è ciclico per il teorema della base normale.

Definizione 3.40. Dato A G-modulo, definiamo il G-modulo

$$A^G := \{a \in A \mid g \cdot a = a \ \forall g \in G\}$$

Diciamo che A è G-modulo banale se $A = A^G$.

Definizione 3.41. Siano A,B G-moduli. $f : A \to B$ è un **omomorfismo di G-moduli** se è un omomorfismo di gruppi e $f(g \cdot a) = g \cdot f(a)$.

Osservazione. Se A, B sono G-moduli, allora lo è anche $\mathrm{Hom}(A, B)$ (inteso come omomorfismi di gruppi abeliani), con l'operazione

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

Inoltre, $\mathrm{Hom}_G(A, B) = (\mathrm{Hom}(A, B))^G$. Un'inclusione è ovvia; supponiamo allora che $f \in \mathrm{Hom}(A, B)^G$. Allora vale che $(g \cdot f)(a) = f(a)$ per ogni $g \in G$. Di conseguenza,

$$\begin{aligned} g(f(a)) &= g \cdot ((g^{-1} \cdot f)(a)) \\ &= f(g(a)) \\ &= f(g \cdot a) \end{aligned}$$

e dunque è un omomorfismo di G-moduli.

Proposizione 3.42. *Sia $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ una successione esatta di G-moduli, dove α e β sono omomorfismi di G-moduli. Allora, posti $\alpha_G = \alpha|_{A^G}$ e $\beta_G = \beta|_{B^G}$, è esatta anche*

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

Dimostrazione. Le restrizioni sono ben definite, in quanto se $a \in A^G$ allora $g\alpha(a) = \alpha(ga) = \alpha(a)$; lo stesso vale per β. Inoltre, α_G è iniettiva in quanto restrizione di mappa iniettiva. Resta da verificare $\mathrm{Im}\,\alpha_G = \mathrm{Ker}\,\beta_G$. Poiché $\beta \circ \alpha = 0$, si ha $\beta_G \circ \alpha_G = 0$ e quindi $\mathrm{Im}\,\alpha_G \subseteq \mathrm{Ker}\,\beta_G$. Mostriamo l'altra inclusione. Sia $y \in \mathrm{Ker}\,\beta_G \subset B^G$: allora $\beta_G(y) = 0$ e per esattezza in B sappiamo che esiste $a \in A$ tale che $y = \alpha(a)$. D'altronde $a \in A^G$; infatti

$$\alpha(ga) = g\alpha(a) = \alpha(a)$$

Per iniettività di α, $ga = a$ e dunque $a \in A^G$. Segue che la successione dei moduli fissati da G è esatta. □

In generale β_G non è surgettiva. Per esempio, consideriamo la successione

$$0 \longrightarrow \langle \zeta_n \rangle \xrightarrow{i} \overline{\mathbb{Q}}^\times \xrightarrow{\beta} \overline{\mathbb{Q}}^\times \longrightarrow 0$$

con $\beta(x) = x^n$. Allora i è iniettiva, $\mathrm{Ker}\,\beta = \mathrm{Im}\,i$ e β è surgettiva (in quanto $\overline{\mathbb{Q}}$ è algebricamente chiuso), dunque la successione è esatta. Inoltre, posto

$G = \mathrm{Gal}(\overline{\mathbb{Q}}^\times/\mathbb{Q}(\zeta_n))$, si ha che $< \zeta_n >$ e $\overline{\mathbb{Q}}^\times$ sono G-moduli e i loro fissati da G sono rispettivamente $< \zeta_n >$ e $\mathbb{Q}(\zeta_n)^\times$. Dunque per la proposizione precedente la successione

$$0 \longrightarrow \langle \zeta_n \rangle \xrightarrow{i} \mathbb{Q}(\zeta_n)^\times \xrightarrow{\beta_G} \mathbb{Q}(\zeta_n)^\times$$

è esatta, ma β_G non è surgettiva, in quanto ζ_n non appartiene all'immagine di β_G.

La mancanza dell'esattezza a destra motiva l'introduzione dei gruppi di coomologia. A tal proposito riprendiamo le definizione di 1-cocicli, 1-cobordi e di primo gruppo di coomologia date in precedenza.

Si noti che se A è G-modulo banale (ossia $A = A^G$), si ha

$$Z^1(G, A) = \mathrm{Hom}(G, A) \qquad\qquad B^1(G, A) = \{0\}$$

Infatti se $f \in Z^1(G, A)$, allora

$$f(\sigma \circ \sigma') = \sigma(f(\sigma'))f(\sigma) \Longrightarrow f(\sigma \circ \sigma') = f(\sigma')f(\sigma)$$

e dunque $f \in \mathrm{Hom}(G, A)$; d'altronde vale anche $\mathrm{Hom}(G, A) \subseteq Z^1(G, A)$. Inoltre, se $f \in B^1(G, A)$, dato che ogni σ agisce banalmente, deve valere che $f(\sigma) = 0$ per ogni $\sigma \in G$ e dunque $f = 0$. Come conseguenza, se A è un G-modulo banale, $H^1(G, A) = \mathrm{Hom}(G, A)$.

Enunciamo il lemma del serpente, che ci servirà per la dimostrazione dell'esistenza della successione esatta lunga in coomologia:

Lemma 3.43 (Snake Lemma)**.** *Si considerino le successioni esatte di A-moduli*

$$M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$
$$0 \longrightarrow M' \xrightarrow{f'} N' \xrightarrow{g'} P'$$

e il diagramma

$$\begin{array}{ccccccc} & & M & \xrightarrow{f} & N & \xrightarrow{g} & P \longrightarrow 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 \longrightarrow & M' & \xrightarrow[f']{} & N' & \xrightarrow[g']{} & P' & \end{array}$$

Se il diagramma commuta, si ha la successione esatta

$$\mathrm{Ker}\,\alpha \to \mathrm{Ker}\,\beta \to \mathrm{Ker}\,\gamma \xrightarrow{\delta} \mathrm{coker}\,\alpha \to \mathrm{coker}\,\beta \to \mathrm{coker}\,\gamma$$

dove $\delta : p \mapsto (m' + \mathrm{Im}\,\alpha)$ con $m' \in M'$ tale che $f'(m') = \beta(n)$ per $n \in g^{-1}(p)$.

Proposizione 3.44. *Data la successione esatta di G-moduli*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

si ha la successione esatta

$$0 \longrightarrow Z^1(G,A) \xrightarrow{f_*} Z^1(G,B) \xrightarrow{g_*} Z^1(G,C)$$

Dimostrazione. Anzitutto f_* e g_* sono ben definite sui codomini. Vediamolo solo per f_*: data $\phi \in Z^1(G,A)$, poniamo $f_*(\phi) = f \circ \phi$ e abbiamo

$$(f \circ \phi)(\sigma \circ \sigma') = f(\phi(\sigma) *_A \sigma\phi(\sigma') = f \circ \phi(\sigma) *_A \sigma(f \circ \phi)(\sigma')$$

e dunque $f_*(\phi) \in Z^1(G,B)$. Vediamo ora l'esattezza della successione:

- f_* é iniettiva: $f_*(\phi) = f \circ \phi \equiv 0 \implies \forall \sigma \in G,\ (f \circ \phi)(\sigma) = 0 \implies \phi(\sigma) \in \operatorname{Ker} f = \{0\} \implies \phi \equiv 0$.
- $\operatorname{Im} f_* \subseteq \operatorname{Ker} g_*$: data $\psi \in \operatorname{Im} f_*$ con $\psi = f_*(\phi)$, $g_*(\psi) = g \circ \psi = g \circ f \circ \phi$, ma $g \circ f = 0$ per esattezza e quindi $g_*(\psi) = 0$.
- $\operatorname{Ker} g_* \subseteq \operatorname{Im} f_*$: $\psi \in \operatorname{Ker} g_* \implies g_*(\psi) = g \circ \psi \equiv 0 \implies \forall \sigma \in G,\ g \circ \psi(\sigma) = 0 \implies \forall \sigma,\ \psi(\sigma) \in \operatorname{Ker} g \overset{\text{ip.}}{=} \operatorname{Im} f \implies \forall \sigma\ \exists a_\sigma$ tale che $\psi(\sigma) = f(a_\sigma)$, ma consideriamo $\phi : \sigma \mapsto a_\sigma$ e abbiamo che $\psi = f_*(\phi)$.

□

Lemma 3.45. *Sia* $0 \to A \to B \to C \to 0$ *successione esatta di G-moduli. Allora é esatta la successione di G-moduli*

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C)$$

Dimostrazione. Consideriamo $\alpha : A \to Z^1(G,A)$ definita da $a \mapsto (f_a : \sigma \mapsto \sigma a - a)$. Allora é facile verificare che $\operatorname{Ker}\alpha = A^G$, $\operatorname{Im}\alpha = B^1(G,A)$ e $\operatorname{coker}\alpha = H^1(G,A)$. Analogamente costruiamo $\beta : B \to Z^1(G,B)$ e $\gamma : C \to Z^1(G,C)$ e otteniamo $\operatorname{Ker}\beta = B^G$, $\operatorname{Ker}\gamma = C^G$, $\operatorname{coker}\beta = H^1(G,B)$ e $\operatorname{coker}\gamma = H^1(G,C)$. Abbiamo dunque il diagramma commutativo

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & Z^1(G,A) & \xrightarrow[f']{} & Z^1(G,B) & \xrightarrow[g']{} & Z^1(G,C) & & \end{array}$$

con le due successioni esatte (la prima per ipotesi, la seconda per la proposizione precedente). Allora per lo Snake Lemma (3.43), é esatta la successione

$$A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C)$$

ed avendo esattezza in A (ossia f iniettiva), si ha che é iniettiva anche $A^G \to B^G$, dunque la tesi. □

Esempio. Data la successione esatta di $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_n))$-moduli

$$0 \longrightarrow \langle\zeta_n\rangle \longrightarrow \overline{\mathbb{Q}}^\times \xrightarrow{(\cdot)^n} \overline{\mathbb{Q}}^\times \longrightarrow 0$$

dal lemma 3.45 si ha che è esatta

$$0 \longrightarrow \langle\zeta_n\rangle \to \mathbb{Q}(\zeta_n)^\times \to \mathbb{Q}(\zeta_n)^\times \to H^1(G, \langle\zeta_n\rangle) \to H^1(G, \overline{\mathbb{Q}}^\times) \to H^1(G, \overline{\mathbb{Q}}^\times)$$

Dato che $\langle\zeta_n\rangle$ è un G-modulo banale, si ha che $H^1(G, \langle\zeta_n\rangle) = \mathrm{Hom}(G, \langle\zeta_n\rangle)$. Invece $H^1(G, \overline{\mathbb{Q}}^\times) = \{1\}$, dunque si la successione esatta

$$0 \longrightarrow \langle\zeta_n\rangle \to \mathbb{Q}(\zeta_n)^\times \to \mathbb{Q}(\zeta_n)^\times \to \mathrm{Hom}(G, \langle\zeta_n\rangle) \to \{1\}$$

e quindi

$$\mathrm{Hom}(G, \langle\zeta_n\rangle) \cong \frac{\mathbb{Q}(\zeta_n)^\times}{(\mathbb{Q}(\zeta_n)^\times)^n}$$

Vediamo ora come la coomologia di gruppi vista finora si ritrova nella coomologia di complessi.

Definizione 3.46. Dato $\mathbb{Z}$ come G-modulo banale, si consideri la risoluzione libera di G-moduli banali per $\mathbb{Z}$

$$\mathcal{P} : \cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

Si dice **complesso** di $\mathcal{P}$

$$\mathcal{K} \coloneqq \mathrm{Hom}(\mathcal{P}, A) : 0 \to \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1} \dots$$

Possiamo dire che la coomologia *misura la mancanza* di esattezza del complesso. Definiamo

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

Considerando la successione esatta $0 \to A \to B \to C \to 0$, abbiamo

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

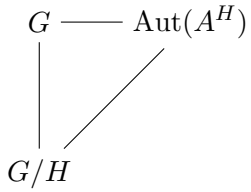
e notiamo che per quanto visto prima si ha $H^0(G, \cdot) = (\cdot)^G$. Posto $N_G = \sum_{\sigma\in G} \sigma$, possiamo definire

$$H^0(G, \cdot) = \frac{(\cdot)^G}{N_G(\cdot)}$$

Sia A un G-modulo e sia $H \triangleleft G$: allora A^H é G-modulo con l'azione

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(A^H) \\ g & \longmapsto & \phi_g|_{A^H} \end{array}$$

Essendo H nel kernel dell'azione, A^H é G/H-modulo con l'azione



Proposizione 3.47. *Siano $H \triangleleft G$ e A G-modulo. Allora è esatta la successione (detta di inflazione e restrizione)*

$$0 \to H^1\left(G/H, A^H\right) \xrightarrow{\psi} H^1(G, A) \xrightarrow{\varphi} H^1(H, A)$$

Dimostrazione. Data $f\colon G/H \to A^H$, definiamo $\psi(f) \in H^1(G, A)$ come composizione di $G \to G/H$ e f. Questo fornisce la prima mappa, che è ben definita. Infatti se $f \in B^1(G/H, A^H)$, allora esiste $a \in A^H$ tale che

$$\overline{f}(\overline{\sigma}) = \overline{\sigma}(a)^{-1}a$$

Allora anche $f \in B^1(G, A)$, in quanto $f(\sigma) = \overline{f}(\overline{\sigma}) = \overline{\sigma}(a)^{-1}a = \sigma(a)^{-1}a$ e questo vale per ogni $\sigma \in G$, da cui la buona definizione. Notiamo che la mappa è banalmente iniettiva. Definiamo ora φ. Questa si ottiene per restrizione di un omomorfismo $f \in Z^1(G, A)$ ad H. Tale mappa passa alla coomologia, in quanto se $f \in B^1(G, A)$, allora chiaramente $f \in B^1(H, A)$. La composizione delle due mappe è nulla; infatti se $\overline{f} \in H^1(G/H, A^H)$, la corrispettiva $f \in H^1(G, A)$ è nulla su H e dunque ha immagine banale. Mostriamo ora che $\ker(\varphi) \subseteq \mathrm{Im}(\psi)$. Sia $f \in Z^1(G, A)$ tale che $f|_H = 0$. Allora esiste $a \in A$ tale che per ogni $\tau \in H$ vale $f(\tau) = \tau(a)^{-1}a$. Notiamo che $a \in A^H$, in quanto f è nulla su H. Definiamo allora $g\colon G \to A$ tale che $g(\sigma) = f(\sigma)a^{-1}\sigma(a)$. Chiaramente $f = g$ in $H^1(G, A)$; inoltre $g(\sigma)$ dipende solo dalla classe di σ modulo H. Infatti se $\tau \in H$,

$$\begin{aligned} g(\sigma\tau) &= f(\sigma\tau)a^{-1}\sigma\tau(a) \\ &= \sigma(f(\tau))f(\sigma)a^{-1}\sigma\tau(a) \\ &= \sigma(\tau(a)^{-1}a)f(\sigma)a^{-1}\sigma\tau(a) \\ &= \sigma(a)f(\sigma)a^{-1} \\ &= g(\sigma) \end{aligned}$$

Sia allora $s\colon G/H \to A^H$ tale che

$$s(\overline{\sigma}) = g(\sigma)$$

Tale mappa è ben definita, perché, dato che g è costante sulle classi laterali di H, si ha

$$\begin{aligned} g(\sigma) &= g(\tau\sigma) \\ &= f(\tau\sigma)a^{-1}(\tau\sigma)(a) \\ &= \tau(f(\sigma))f(\tau)a^{-1}(\tau\sigma)(a) \\ &= \tau(f(\sigma)a\sigma(a)^{-1}) \\ &= \tau g(\sigma) \end{aligned}$$

□

3.5 Teoria di Kummer

Sia K un campo con le radici n-esime dell'unità di caratteristica $p \nmid n$. Sia $U_n = \langle \zeta_n \rangle \subseteq \mathbb{C}^\times$. Sappiamo già che se L/K è ciclica di grado n, esiste $a \in K$ tale che $L = K(\sqrt[n]{a})$. Viceversa, se $a \in K$, $L = K(\sqrt[n]{a})$ è ciclica di grado $d \mid n$. Un esempio di questo caso sono le estensioni quadratiche di un campo qualsiasi (di caratteristica diversa da 2). Sappiamo per queste estensioni che $K(\sqrt{a}) = K(\sqrt{b})$ se e solo se $a \in b(K^\times)^2$. Estendiamo allora il caso ciclico al caso abeliano; per questo, introduciamo la seguente classe di estensioni:

Definizione 3.48. Sia L/K un'estensione abeliana. L/K si dice **di Kummer** se è di esponente finito n tale che $\zeta_n \in K$, $\operatorname{char} K \nmid n$.

Generalizziamo i risultati sulle estensioni cicliche alle estensioni di Kummer, non necessariamente finite:

Proposizione 3.49. *Sia K un campo di caratteristica $p \nmid n$ e sia $L = K(\sqrt[n]{\Delta})$, dove Δ è un sottoinsieme di K. Allora L/K è di Kummer di esponente n.*

Dimostrazione. Chiaramente l'estensione è di Galois, in quanto campo di spezzamento dei polinomi separabili $x^n - a$, $a \in \Delta$. Sappiamo che il gruppo

$$\operatorname{Gal}\left(K(\sqrt[n]{a})/K\right)$$

è ciclico di ordine $d \mid n$ per il teorema 3.6. Per ogni $a \in \Delta$ la restrizione

$$\operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}\left(K(\sqrt[n]{a})/K\right)$$

è un omomorfismo di gruppi e questi inducono una mappa sul prodotto

$$\varphi\colon \operatorname{Gal}(L/K) \longrightarrow \prod_{a\in\Delta} \operatorname{Gal}\left(K(\sqrt[n]{a})/K\right)$$

Il prodotto è abeliano ed è di esponente n e inoltre φ è iniettivo perché L è il composto dei campi $K(\sqrt[n]{a})$, da cui la tesi. □

Proposizione 3.50. *Sia L/K un'estensione di Kummer di esponente n. Allora $L = K(\sqrt[n]{\Delta})$, dove $\Delta = (L^\times)^n \cap K^\times$.*

Dimostrazione. Sicuramente $K(\sqrt[n]{\Delta}) \subseteq L$; mostriamo l'inclusione opposta. Notiamo che $L = \prod L_i$ è il composto di tutte le sue sottoestensioni finite e abeliane di esponente n. Per il teorema di struttura dei gruppi abeliani, $\mathrm{Gal}(L_i/K)$ si decompone come prodotto diretto di gruppi ciclici di ordine $d \mid n$. Dunque $L_i = \prod F_{ij}$ è composto delle sue sottoestensioni cicliche. Di conseguenza

$$L = \prod_{i,j} F_{ij}$$

Per il teorema 3.6, esiste $a \in K^\times$ tale che $F_{ij} = K(\sqrt[n]{a})$. Da questo si deduce anche che $a \in (L^\times)^n$ e dunque $a \in \Delta$. Da questo segue che L è generato da elementi di Δ, da cui la tesi. □

Studiamo ora la struttura di $(L^\times)^n \cap K^\times$ dove $L = K(\sqrt[n]{a})$. Supponiamo per semplicità che L/K sia ciclica di grado n e in particolare che $a \notin (K^\times)^d$ per ogni $d \mid n$. Possiamo scegliere in questo caso un generatore σ di $\mathrm{Gal}(L/K)$ tale che $\sigma(\sqrt[n]{a}) = \zeta_n \sqrt[n]{a}$. Allora

$$(L^\times)^n \cap K = \bigsqcup_{i=0}^{n-1} a^i (K^\times)^n$$

Intanto l'unione è disgiunta, in quanto a non è una potenza d-esima per ogni $d \mid n$. Sia $b \in (L^n) \cap K^\times$; allora $\sqrt[n]{b} = \beta \in L$. Dunque

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i$$

Applicando σ,

$$\sigma(\beta) = b_0 + b_1 \zeta \alpha + \cdots + b_{n-1} \zeta^{n-1} \alpha^{n-1}$$

Dato che β è radice di $x^n - b$, si ha che $\sigma(\beta)$ è una radice di $x^n - b$, da cui

$$\sigma(\beta) = \zeta^h \beta = \sum b_i \zeta^h \alpha^i$$

Uguagliando le due espressioni,

$$0 = b_0(\zeta^h - 1)\alpha + b_1(\zeta^h - \zeta)\alpha + \cdots + b_{n-1}(\zeta^h - \zeta^{n-1})\alpha^{n-1}$$

Dunque ogni coefficiente deve essere 0 e $b_i = 0$ per ogni $i \neq h$ e $b_h \neq 0$. Dunque $b = \beta^n = b_h^n a^h$ e $b \in (K^\times)^n a^h$, come voluto.

Esempio. Vediamo quando $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$. Questo vale se e solo se

$$\bigcup a^i (K^\times)^i = \bigcup b^i (K^\times)^i$$

e dato che sono disgiunte, esiste k con $(k,n) = 1$ tale che $a \in (K^\times)^n b^k$. Questo è equivalente a dire che $\langle a(K^\times)^n \rangle = \langle b(K^\times)^n \rangle$ in $K^\times/(K^\times)^n$.

Dunque siamo in grado di individuare per ogni estensione di Kummer un sottogruppo di $K^\times$ e viceversa. In effetti, esiste una corrispondenza biunivoca tra queste.

Teorema 3.51 (Kummer)**.** *Sia K un campo tale che* $\operatorname{char} K \nmid n$*. Le estensioni abeliane di esponente n sono in corrispondenza biunivoca con i sottogruppi di $K^\times$ che contengono $(K^\times)^n$.*

$$\begin{array}{ccc} \{\textit{estensioni abeliane di esponente } n\} & \longleftrightarrow & \{\Delta \mid (K^\times)^n \subseteq \Delta \subseteq K^\times\} \\ L & \xrightarrow{\alpha} & (L^\times)^n \cap K \\ K(\sqrt[n]{\Delta}) & \xleftarrow{\beta} & \Delta \end{array}$$

Inoltre, esiste un isomorfismo canonico

$$\begin{array}{rccc} \psi\colon & \Delta/K^{\times n} & \longrightarrow & \operatorname{Hom}_{cont}(\operatorname{Gal}(L/K), \langle\zeta_n\rangle) \\ & a K^{\times n} & \longmapsto & \chi_a\colon \operatorname{Gal}(L/K) \longrightarrow \langle\zeta_n\rangle \\ & & & \sigma \longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array}$$

Osservazione. Gli omomorfismi χ sono caratteri e se G è abeliano di esponente n allora $\chi(G) \subseteq \langle\zeta_n\rangle$. Dunque questi sono tutti e soli i caratteri di G.

Notiamo che $K(\sqrt[n]{a})$ è la massima estensione abeliana di esponente n di K.

Dimostrazione. Sia L/K abeliana di esponente n. Detto $\Delta = L^{\times n} \cap K^\times$, sappiamo che $L = K(\sqrt[n]{\Delta})$. Costruiamo la ψ, come nell'enunciato, definendola su Δ. Mostriamo che ψ è ben definita, ossia che χ è continuo. Basta mostrare che la controimmagine di 1 è un aperto di G, perché $\langle\zeta_n\rangle$ ha la topologia discreta. ma $\chi^{-1}(1) = \operatorname{Gal}(L/K(\sqrt[n]{a}))$, da cui la continuità. ψ è un omomorfismo e

$$\ker(\psi) = \{a \in \Delta \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\} = K^{\times n}$$

da cui otteniamo il passaggio al quoziente. Mostriamo che ψ è surgettiva. Supponiamo dapprima che G sia finito. Consideriamo la successione esatta corta di G-moduli

$$0 \to \langle\zeta_n\rangle \longrightarrow L^\times \xrightarrow{(\cdot)^n} (L^\times)^n \to 0$$

Passando in coomologia, poiché L/K è finita, per il teorema di Hilbert 90,

$$0 \to \langle \zeta_n \rangle \longrightarrow K^\times \longrightarrow (L^\times)^n \cap K^\times \xrightarrow{\delta} H^1(G, \langle \zeta_n \rangle) \longrightarrow \{1\}$$

Dato che $\langle \zeta_n \rangle$ è un G-modulo banale, $H^1(G, \langle \zeta_n \rangle) = Hom(G, \langle \zeta_n \rangle)$ e otteniamo un l'isomorfismo

$$(L^\times)^n \cap K^\times \big/ (K^\times)^n \longrightarrow \mathrm{Hom}(G, \langle \zeta_n \rangle)$$

che risulta essere proprio quello indicato nell'enunciato (basta ripercorrere la dimostrazione del lemma del serpente).

Se G è infinito, possiamo scrivere $L = \cup L_i$ unione delle sottoestensioni finite e per ogni sottoestensione vale l'isomorfismo. Sia $\chi \in \mathrm{Hom}(G, < \zeta_n >)$ e verifichiamo che appartiene all'immagine. Notiamo che $\ker(\chi)$ è un sottogruppo aperto di G. Allora esiste i tale che

$$\mathrm{Gal}(L_i/K) \subseteq \ker(\chi)$$

dunque l'omomorfismo passa al quoziente. Ossia otteniamo

$$\overline{\chi} : G \big/ \mathrm{Gal}(L/L_i) \longrightarrow \langle \zeta_n \rangle$$

Dato che sul quoziente sappiamo che la tesi è vera (è un gruppo finito), esiste $a \in \Delta_i$ tale che $\overline{\chi} = \chi_a$. Allora $\chi(\sigma) = \overline{\chi}(\sigma|_{L_i}) = \chi_a(\sigma|_{L_i}) = \chi_a(\sigma)$. □

Diamo ora dei risultati che ci serviranno per concludere la dimostrazione. Sia G un gruppo abeliano finito. Possiamo considerare il gruppo

$$\hat{G} = \mathrm{Hom}(G, \mathbb{C})$$

di tutti i caratteri di G.

Lemma 3.52. $\hat{G} \simeq G$

Dimostrazione. Se G è ciclico, sappiamo che

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^*) \simeq \mathbb{Z}/n\mathbb{Z}$$

Dunque per il teorema di struttura, poichè $G \simeq \oplus \mathbb{Z}/n_i\mathbb{Z}$, si ha

$$\hat{G} = \mathrm{Hom}(\oplus \mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*) \simeq \oplus \,\mathrm{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*).$$

□

Lemma 3.53. *Sia G abeliano finito. Allora $\hat{\hat{G}} \simeq G$ in modo canonico.*

Dimostrazione. Consideriamo l'omomorfismo

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathrm{Hom}(\hat{G}, \mathbb{C}^*) \\ & g & \longmapsto & \chi \mapsto \chi(g) \end{array}$$

Mostriamo l'iniettività.Supponiamo che g sia tale che $\chi(g) = 1$ per ogni $\chi \in \hat{G}$. Allora $H = \ker(\varphi) = \{g \in G \mid \chi(g) = 1 \, \forall \chi \in \hat{G}\}$. Tali omomorfismi passano al quoziente, ossia $\varphi \in \hat{G/H}$. Dunque $\hat{G} \subseteq \hat{G/H}$ e questo è possibile se e solo se $H = \{e\}$ per questioni di cardinalità. Ora, dato che G e $\hat{\hat{G}}$ hanno la stessa cardinalità, sono isomorfi. □

Consideriamo l'accoppiamento di dualità

$$\begin{array}{ccc} G \times G & \longrightarrow & \mathbb{C}^* \\ (g, \chi) & \longmapsto & \chi(g) \end{array}$$

Questo non è degenere, perché se $\chi(g) = 1$ per ogni $g \in G$ allora $\chi = 1$ e se $\chi(g) = 1$ per ogni $\chi \in \hat{G}$, $\chi = 1$. Possiamo allora considerare l'ortogonale di un sottoinsieme $H \subseteq G$, ossia

$$H^\perp = \{\chi \in \hat{G} \mid \chi(h) = 1 \, \forall h \in G\} < \hat{G}.$$

Allo stesso modo, dato $X \subseteq \hat{G}$,

$$X^\perp = \{h \in G \mid \chi(h) = 1 \, \forall \chi \in X\} = \bigcap_{\chi \in X} \ker(\chi) < G.$$

Sicuramente se H è un sottogruppo, $H^\perp \simeq \hat{G/H}$ (basta mandare $\chi \mapsto \bar{\chi}$, perché χ passa al quoziente su H.

Notiamo anche che, dato $H < G$, si ha $H^{\perp\perp} = H$. Infatti

$$(H^\perp)^\perp = \{g \in G \mid \chi(g) = 1 \, \forall \chi \in H^\perp\},$$

in particolare, $H \subseteq (H^\perp)^\perp$. Inoltre,

$$|H^\perp| = \left|\hat{G/H}\right| = \left|G/H\right|$$

e dunque $|H||H^\perp| = |G|$. Applicando questa formula a $(H^\perp)^\perp$, si ha la tesi.

In questo modo, abbiamo trovato una corrispondenza tra i sottogruppi di G e quelli di $\hat{G}$. Nel caso dei gruppi di Galois, questo ci dice che, preso $G = \mathrm{Gal}(L/K)$ abeliano finito, ai sottogruppi di $\hat{G}$ corrispondono sottogruppi di G, che a loro volta corrispondono alle sottoestensioni di L/K. In particolare, G corrisponde a L.

Riprendiamo ora la dimostrazione del teorema di Kummer.

Dimostrazione. Vediamo la corrispondenza biunivoca. Chiaramente $\beta \circ \alpha =$ id. Mostriamo il viceversa,

$$\alpha \circ \beta(\Delta) = L^{\times n} \cap K^{\times} = \Delta'$$

Chiaramente vale $\Delta \subseteq \Delta'$. Inoltre per ipotesi $K^{\times n} \subseteq \Delta \subseteq K^{\times}$. Supponiamo dapprima che L/K sia finita. Sappiamo che ${}^{\Delta'}\!/_{K^{\times n}} \cong \mathrm{Hom}(G, \langle \zeta_n \rangle)$. Se per assurdo $\Delta \subsetneq \Delta'$, allora ${}^{\Delta}\!/_{K^{\times n}}$ è un sottogruppo proprio di ${}^{\Delta}\!/_{K^{\times n}}$. Dunque corrisponde a $X = \{\chi_a | a \in \Delta\}$, sottogruppo proprio di $\mathrm{Hom}(G, \langle \zeta_n \rangle)$. Vediamo chi è il suo ortogonale:

$$\begin{aligned} X^{\perp} &= \{\sigma \in G \mid \chi_a(\sigma) = 1 \, \forall a \in \Delta\} \\ &= \{\sigma \in G \mid \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \, \forall a \in \Delta\} \\ &= \{\mathrm{id}\} \end{aligned}$$

Ma allora $X = \hat{G} = \mathrm{Hom}(G, \langle \zeta_n \rangle)$, assurdo.
Se invece L/K è infinita, $\Delta = \cup_{i \in I} \Delta_i$, dove

$$\{\Delta_i\}_{i \in I} = \{\Delta_i \subseteq \Delta \mid {}^{\Delta}\!/_{K^{\times n}} \text{ finito}\}$$

Posto $L_i = K(\sqrt[n]{\Delta_i})$, in questo caso $\Delta_i' = \Delta_i = L_i^{\times n} \cap K^{\times n}$. Dunque $L = \bigcup_{i \in I} K(\sqrt[n]{\Delta_i}) = \bigcup_{i \in I} L_i$ ed inoltre $L^{\times n} = \bigcup_{i \in I} L_i^{\times n}$. Ma allora:

$$\Delta' = L^{\times n} \cap K^{\times n} = \cup_{i \in I} L_i^{\times n} \cap K^{\times n} = \cup_{i \in I} \Delta_i' = \cup_{i \in I} \Delta_i = \Delta$$

□

Teorema 3.54 (di Albert)**.** *Sia $p \in \mathbb{Z}$ un primo e sia K un campo di caratteristica $\neq p$. Supponiamo che $\zeta_{p^e} \in K$ per un certo $e \geq 1$. Sia L/K ciclica di grado p^r, con $r \geq 0$. Allora esiste un'estensione M/K tale che $M \supseteq L$ ciclica di grado $[M : K] = p^{e+r}$ se e solo se esiste $y \in L^{\times}$ tale che $\mathrm{N}_{L/K}(y) = \zeta_{p^e}$. In tal caso, esiste $z \in L^{\times}$ tale che $M = L(\sqrt[p^e]{z})$ e $y = \tau(\sqrt[p^e]{z})/\sqrt[p^e]{z}$ per un τ tale che $\langle \tau \rangle = \mathrm{Gal}(M/K)$.*