# Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2020/2021
Teoria dei campi

# Testi di riferimento

Per la parte di teoria dei campi potranno essere utili in particolare i seguenti testi.

- D.J.H. Garling, *A Course in Galois Theory*
  Soprattutto i capitoli 4 e 7-12.
- J.S. Milne, *Fields and Galois Theory*, disponibile all'indirizzo
  `http://www.jmilne.org/math/CourseNotes/ft.html`
  Soprattutto i capitoli 1-3.
- I.N. Herstein, *Algebra*
  Capitolo 5.
- Dispense di R. Schoof e B. van Geemen, disponibili all'indirizzo
  `http://www-dimat.unipv.it/canonaco/notealgebra.pdf`
  Capitolo 14.

# Caratteristica di un anello

## Definizione

La caratteristica di un anello $A$ è $\mathrm{char}(A) \in \mathbb{N}$ tale che, se $f : \mathbb{Z} \to A$ indica l'unico omomorfismo di anelli, $\mathrm{char}(A)\mathbb{Z} = \ker(f)$.

## Esempio

$\mathrm{char}(\mathbb{Z}) = 0$ e $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n \ \forall\, n > 0$.
$\mathrm{char}(A) = \mathrm{char}(B)$ se $\exists\, A \to B$ omomorfismo iniettivo di anelli.

## Osservazione

$\mathrm{im}(f) \cong \mathbb{Z}/\mathrm{char}(A)\mathbb{Z}$ per il primo teorema di isomorfismo.

- Poiché $\mathrm{im}(f) = \{n_A \,:\, n \in \mathbb{Z}\} = \langle 1_A \rangle$,

$$\mathrm{char}(A) = \begin{cases} \mathrm{ord}(1_A) & \text{se } \mathrm{ord}(1_A) < \infty \\ 0 & \text{se } \mathrm{ord}(1_A) = \infty. \end{cases}$$

- $A$ dominio (in particolare campo) $\implies$ $\mathrm{im}(f)$ dominio $\implies$ $\mathrm{char}(A)\mathbb{Z}$ ideale primo $\implies$ $\mathrm{char}(A)$ è 0 o un numero primo.

# Campo dei quozienti di un dominio

Indichiamo con $Q(A)$ il campo dei quozienti (o delle frazioni) di un dominio $A$. Vediamo $A$ come sottoanello di $Q(A)$ identificando $a \in A$ con $a/1 \in Q(A)$.

## Lemma

*$f : A \to K$ omomorfismo iniettivo di anelli con $A$ dominio e $K$ campo $\implies \exists!\, \tilde{f} : Q(A) \to K$ omomorfismo di anelli tale che $\tilde{f}|_A = f$; inoltre $\tilde{f}$ è iniettivo.*

## Corollario

*$K$ campo tale che $\mathrm{char}(K) = 0 \implies \exists!\, \mathbb{Q} \to K$ omomorfismo (iniettivo) di anelli.*

## Dimostrazione.

$\exists!\, f : \mathbb{Z} \to K$ omomorfismo di anelli, e $f$ è iniettivo perché $\mathrm{char}(K) = 0$. Per il Lemma $\exists!\, \tilde{f} : Q(\mathbb{Z}) = \mathbb{Q} \to K$ omomorfismo (iniettivo) di anelli (tale che $\tilde{f}|_{\mathbb{Z}} = f$). □

# Dimostrazione del Lemma

- unicità: $\tilde{f}(a/b) = \tilde{f}(ab^{-1}) = \tilde{f}(a)\tilde{f}(b)^{-1} = f(a)f(b)^{-1}$ $\forall\, a \in A, \forall\, b \in A \setminus \{0\}$.
- $\tilde{f}(a/b) := f(a)f(b)^{-1}$ $\forall\, a \in A, \forall\, b \in A \setminus \{0\}$ è ben definito: $f(b) \in K \setminus \{0\} = K^*$ perché $f$ iniettivo; $a/b = a'/b'$ (con $a', b' \in A$ e $b' \neq 0$) $\implies$ $ab' = a'b$ $\implies$ $f(ab') = f(a'b)$ $\implies$ $f(a)f(b') = f(a')f(b)$ $\implies$ $f(a)f(b)^{-1} = f(a')f(b')^{-1}$.
- $\tilde{f}$ è un omomorfismo di anelli: $\forall\, a, c \in A$ e $\forall\, b, d \in A \setminus \{0\}$ $\tilde{f}((a/b)+(c/d)) = \tilde{f}((ad+bc)/(bd)) = f(ad+bc)f(bd)^{-1} = f(a)f(b)^{-1} + f(c)f(d)^{-1} = \tilde{f}(a/b) + \tilde{f}(c/d)$; $\tilde{f}((a/b)(c/d)) = \tilde{f}((ac)/(bd)) = f(ac)f(bd)^{-1} = f(a)f(b)^{-1}f(c)f(d)^{-1} = \tilde{f}(a/b)\tilde{f}(c/d)$; $\tilde{f}(1_{Q(A)}) = f(1_A) = 1_K$.
- $\tilde{f}|_A = f$ perché $\tilde{f}(a) = \tilde{f}(a/1) = f(a)f(1)^{-1} = f(a)$ $\forall\, a \in A$.
- $\tilde{f}$ iniettivo perché $Q(A)$ è un campo e $K \neq \{0\}$.

# Sottocampi

## Definizione

Se $K$ è un campo, $F \subseteq K$ è un sottocampo di $K$ se $F$ è un sottoanello di $K$ e come anello è un campo.

Chiaramente $F \subseteq K$ è un sottocampo di $K \iff$

- $1 \in F$;
- $a, b \in F \implies a - b, ab \in F$;
- $a \in F \setminus \{0\} \implies a^{-1} \in F$.

## Esempio

Le seguenti inclusioni sono sottocampi:

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$;
- $K \subset K(X) := Q(K[X])$ $\forall\, K$ campo.

## Osservazione

$K$ campo, $F_\lambda \subseteq K$ sottocampi (con $\lambda \in \Lambda$) $\implies \bigcap_{\lambda \in \Lambda} F_\lambda \subseteq K$ sottocampo (esercizio).

# Sottocampo primo di un campo

## Definizione

Il sottocampo primo di un campo $K$ è il più piccolo sottocampo di $K$, cioè l'intersezione di tutti i sottocampi di $K$.

## Proposizione

*$K$ campo, $F \subseteq K$ sottocampo primo di $K$* $\implies$

$$F \cong \begin{cases} \mathbb{Q} & \text{se } \operatorname{char}(K) = 0 \\ \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} & \text{se } \operatorname{char}(K) = p \text{ primo.} \end{cases}$$

## Dimostrazione.

$f : \mathbb{Z} \to F$ unico omomorfismo di anelli, $c := \operatorname{char}(K) = \operatorname{char}(F)$.

- $c = p \implies$ per il primo teorema di isomorfismo per anelli $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker(f) \cong \operatorname{im}(f) \subseteq F$ sottocampo $\implies \operatorname{im}(f) = F$.
- $c = 0 \implies$ per il Corollario $\exists\ \tilde{f} : \mathbb{Q} \to F$ omomorfismo iniettivo $\implies \mathbb{Q} \cong \operatorname{im}(\tilde{f}) \subseteq F$ sottocampo $\implies \operatorname{im}(\tilde{f}) = F$.

# Estensioni di campi

### Definizione

Un'estensione di campi è un omomorfismo (necessariamente iniettivo) di anelli $K \to L$ con $K$ e $L$ campi.

### Esempio

$L$ campo, $K \subseteq L$ sottocampo $\implies$ l'omomorfismo di inclusione $K \to L$ è un'estensione di campi.

### Osservazione

Sia $i\colon K \to L$ è un'estensione di campi.

- $L$ è una $K$-algebra, e in particolare un $K$-spazio vettoriale.
- $K' := \mathrm{im}(i) \subseteq L$ sottocampo tale che $K \cong K'$.

Per abuso di notazione, spesso un'estensione di campi $i\colon K \to L$ viene indicata semplicemente con $K \subseteq L$, anche quando $i$ non è un'inclusione. Tale abuso verrà evitato quando $i$ sarà rilevante.

# Grado di un'estensione di campi

## Definizione

Il grado di un'estensione di campi $K \subseteq L$ è

$$[L : K] := \dim_K(L).$$

L'estensione si dice finita se $[L : K] < \infty$.

Se $K \subseteq L$ non è finita, scriveremo semplicemente $[L : K] = \infty$.

## Osservazione

- $[L : K]$ non va confuso con l'indice di $K < L$.
- $[L : K] > 0$ e $[L : K] = 1 \iff K = L$.

## Esempio

- $[\mathbb{C} : \mathbb{R}] = 2$ perché $\{1, i\}$ è una $\mathbb{R}$-base di $\mathbb{C}$.
- $[K(X) : K] = \infty$ perché $\{X^n : n \in \mathbb{N}\} \subset K[X] \subset K(X)$ è $K$-linearmente indipendente.

# Proprietà delle estensioni finite

## Proposizione

*$F \subseteq K \subseteq L$ estensioni. Allora $F \subseteq L$ è finita $\iff$ $F \subseteq K$ e $K \subseteq L$ sono finite. Inoltre in tal caso* $[L : F] = [L : K][K : F]$.

## Dimostrazione.

$[K : F] \leq [L : F]$ (perché $K$ è un $F$-sottospazio vettoriale di $L$) e $[L : K] \leq [L : F]$ (perché ogni insieme di generatori di $L$ su $F$ lo è anche su $K$), dunque basta dimostrare l'ultima affermazione.
$[K : F] = m$ e $[L : K] = n \implies K \cong F^m$ come $F$-spazi vettoriali e $L \cong K^n$ come $K$- e quindi anche come $F$-spazi vettoriali $\implies$ $L \cong (F^m)^n \cong F^{mn}$ come $F$-spazi vettoriali $\implies [L : F] = mn$. □

## Osservazione

$\{\alpha_1, \ldots, \alpha_m\}$ $F$-base di $K$ e $\{\beta_1, \ldots, \beta_n\}$ $K$-base di $L \implies$ $\{\alpha_i\beta_j : i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ $F$-base di $L$: basta dimostrare che è un insieme di generatori, il che è vero perché ogni elemento di $L$ è della forma $\sum_{j=1}^{n} b_j\beta_j$ con $b_j = \sum_{i=1}^{m} a_{i,j}\alpha_i$ e $a_{i,j} \in F$.

# Estensione generata da un sottoinsieme

- $B$ anello commutativo, $A \subseteq B$ sottoanello, $U \subseteq B \implies$
  $A[U]$ indica il più piccolo sottoanello di $B$ contenente $A$ e $U$, cioè l'intersezione di tutti i sottoanelli di $B$ contenenti $A$ e $U$.
  Inoltre è facile vedere che

  $$A[U] = \{f(b_1, \ldots, b_n) \,:\, f \in A[X_1, \ldots, X_n],\ b_1, \ldots, b_n \in U\}.$$

  In particolare $A[b] := A[\{b\}] = \{f(b) \,:\, f \in A[X]\}\ \forall\, b \in B$.
- $K \subseteq L$ estensione, $U \subseteq L$ sottoinsieme $\implies$
  $K(U)$ indica il più piccolo sottocampo di $L$ contenente $K$ e $U$, cioè l'intersezione di tutti i sottocampi di $L$ contenenti $K$ e $U$.
  Chiaramente $K[U] \subseteq K(U)$ e è facile vedere che

  $$K(U) = \left\{\alpha\beta^{-1} \,:\, \alpha, \beta \in K[U],\ \beta \neq 0\right\} \cong Q(K[U])$$

  (l'inclusione $K[U] \to K(U)$ si estende a un omomorfismo iniettivo $Q(K[U]) \to K(U)$, che è anche suriettivo).
  Ovviamente $K \subseteq K(U)$ è un'estensione, detta generata da $U$ (su $K$).

# Estensioni finitamente generate e estensioni semplici

## Definizione

Un'estensione $K \subseteq L$ è finitamente generata se $\exists\, U \subseteq L$ finito tale che $L = K(U)$. L'estensione è semplice se $\exists\, \alpha \in L$ tale che $L = K(\alpha) := K(\{\alpha\})$.

## Esempio

Un'estensione $K \subseteq L$ è semplice se $[L : K] = p$ primo: date estensioni $K \subseteq K' \subseteq L$, da

$$p = [L : K] = [L : K'][K' : K]$$

segue $[L : K'] = 1$ e $[K' : K] = p$ o $[L : K'] = p$ e $[K' : K] = 1$, e quindi $K' = L$ o $K' = K$.
Allora $L = K(\alpha)\ \forall\, \alpha \in L \setminus K$.

# Elementi algebrici e elementi trascendenti

## Definizione

$K \subseteq L$ estensione. Si dice che $\alpha \in L$ è algebrico su $K$ se $\exists\, 0 \neq f \in K[X]$ tale che $f(\alpha) = 0$.
Altrimenti si dice che $\alpha$ è trascendente su $K$.

## Proposizione

*$K \subseteq L$ estensione, $\alpha \in L$.*

1. *$\alpha$ trascendente su $K$ $\implies$ $K[\alpha] \cong K[X]$ e $K(\alpha) \cong K(X)$ come $K$-algebre.*
2. *$\alpha$ algebrico su $K$ $\implies$ $\exists!\, \mathrm{m}_\alpha = \mathrm{m}_{\alpha,K} \in K[X]$ monico (detto polinomio minimo di $\alpha$ su $K$) tale che*

$$\{f \in K[X] \,:\, f(\alpha) = 0\} = (\mathrm{m}_\alpha).$$

*Inoltre $\mathrm{m}_\alpha$ è irriducibile in $K[X]$ e $K[\alpha] = K(\alpha) \cong K[X]/(\mathrm{m}_\alpha)$ come $K$-algebre.*

# Dimostrazione della Proposizione

$g\colon K[X] \to L$, $f \mapsto f(\alpha)$ è un omomorfismo di $K$-algebre (è l'unico tale che $X \mapsto \alpha$); inoltre $\mathrm{im}(g) = \{f(\alpha) : f \in K[X]\} = K[\alpha]$ e $\ker(g) = \{f \in K[X] : f(\alpha) = 0\}$.

1. $\ker(g) = \{0\} \implies K[X] \cong \mathrm{im}(g) = K[\alpha]$ (come $K$-algebre), quindi anche $K(X) = Q(K[X]) \cong Q(K[\alpha]) \cong K(\alpha)$.
2. $\ker(g)$ ideale non nullo di $K[X]$ dominio a ideali principali tale che $K[X]^* = K^* \implies \exists!\, \mathrm{m}_\alpha \in K[X]$ monico tale che $\ker(g) = (\mathrm{m}_\alpha) \implies$ per il primo teorema di isomorfismo

$$K[\alpha] = \mathrm{im}(g) \cong K[X]/\ker(g) = K[X]/(\mathrm{m}_\alpha)$$

come anelli, ma è facile vedere che l'isomorfismo (essendo indotto da $g$) è anche di $K$-algebre.
$K[\alpha] \subseteq L$ sottoanello $\implies K[\alpha] \cong K[X]/(\mathrm{m}_\alpha)$ dominio $\implies$ $(\mathrm{m}_\alpha)$ ideale primo non nullo $\implies \mathrm{m}_\alpha$ irriducibile e $(\mathrm{m}_\alpha)$ ideale massimale $\implies K[\alpha] \cong K[X]/(\mathrm{m}_\alpha)$ campo $\implies$ $K[\alpha] = K(\alpha)$ (dato che in ogni caso $K[\alpha] \subseteq K(\alpha)$).

# Grado di un'estensione semplice

**Lemma**

$0 \neq f \in K[X] \implies \dim_K(K[X]/(f)) = \deg(f)$.

**Corollario**

*$K \subseteq L$ estensione, $\alpha \in L \implies$ sono equivalenti:*

1. *$\alpha$ è algebrico su $K$;*
2. *$K[\alpha] = K(\alpha)$;*
3. *$[K(\alpha) : K] < \infty$, e in questo caso $[K(\alpha) : K] = \deg(\mathrm{m}_\alpha)$.*

**Dimostrazione.**

1 $\implies$ 2 Per la parte 2 della Proposizione.

2 $\implies$ 3 $K[\alpha] = K(\alpha)$ campo $\implies$ $K[\alpha] \not\cong K[X] \implies$
$\alpha$ algebrico su $K$ per la parte 1 della Proposizione $\implies$
$K(\alpha) \cong K[X]/(\mathrm{m}_\alpha)$ per la parte 2 della Proposizione $\implies$
$[K(\alpha) : K] = \dim_K(K[X]/(\mathrm{m}_\alpha)) = \deg(\mathrm{m}_\alpha)$ per il Lemma.

3 $\implies$ 1 Per la parte 1 della Proposizione, dato che $\dim_K(K(X)) = \infty$.

# Dimostrazione del Lemma

- $d := \deg(f)$, $K[X]_{<d} := \{g \in K[X] \,:\, g = 0 \text{ o } \deg(g) < d\}$ $K$-sottospazio vettoriale di $K[X]$ tale che $\dim_K(K[X]_{<d}) = d$ (una base di $K[X]_{<d}$ è $\{X^i \,:\, 0 \leq i < d\}$).
- La funzione

$$\psi \colon K[X] \to K[X]$$
$$g \mapsto r \text{ con } g = qf + r,\ q \in K[X] \text{ e } r \in K[X]_{<d}$$

  è ben definita e $K$-lineare (esercizio).
- $\mathrm{im}(\psi) = K[X]_{<d}$ (perché $\psi(g) = g$ se $g \in K[X]_{<d}$) e $\ker(\psi) = \{qf \,:\, q \in K[X]\} = (f) \implies$

$$K[X]/(f) = K[X]/\ker(\psi) \cong \mathrm{im}(\psi) = K[X]_{<d}$$

  come $K$-spazi vettoriali per il primo teorema di isomorfismo $\implies \dim_K(K[X]/(f)) = \dim_K(K[X]_{<d}) = d$.

## Osservazione

Una $K$-base di $K[X]/(f)$ è $\{X^i + (f) \,:\, 0 \leq i < d\}$.

# Estensioni algebriche e estensioni finite

## Definizione

Un'estensione $K \subseteq L$ è algebrica se $\alpha$ è algebrico su $K$ $\forall\, \alpha \in L$.

## Proposizione

*$K \subseteq L$ estensione $\implies$ sono equivalenti:*

1. *$K \subseteq L$ è finita;*
2. *$K \subseteq L$ è algebrica e finitamente generata;*
3. *$\exists\, \alpha_1, \ldots, \alpha_n \in L$ algebrici su $K$ tali che $L = K(\alpha_1, \ldots, \alpha_n)$.*

## Dimostrazione.

$1 \implies 2$ $\alpha \in L \implies [K(\alpha) : K] \leq [L : K] < \infty \implies \alpha$ algebrico su $K$.
$L = \langle \alpha_1, \ldots, \alpha_n \rangle_K \implies L = K(\alpha_1, \ldots, \alpha_n)$.

$2 \implies 3$ Chiaro.

$3 \implies 1$ $\alpha_i$ algebrico su $K \implies \alpha_i$ algebrico su $K_i := K(\alpha_1, \ldots, \alpha_{i-1})$
$\implies [K_{i+1} = K_i(\alpha_i) : K_i] < \infty \;\forall\, i = 1, \ldots, n \implies$
$[L : K] = \prod_{i=1}^{n} [K_{i+1} : K_i] < \infty$.

# Proprietà delle estensioni algebriche

## Osservazione

$K \subseteq K' \subseteq L$ estensioni, $\alpha \in L$ algebrico su $K \implies$ $\alpha$ algebrico su $K'$ e $[K'(\alpha) : K'] \leq [K(\alpha) : K] < \infty$: $\mathrm{m}_{\alpha,K} \in K[X] \subseteq K'[X]$ tale che $\mathrm{m}_{\alpha,K}(\alpha) = 0 \implies \mathrm{m}_{\alpha,K'} \mid \mathrm{m}_{\alpha,K}$ in $K'[X] \implies \deg(\mathrm{m}_{\alpha,K'}) \leq \deg(\mathrm{m}_{\alpha,K})$.

## Proposizione

*$F \subseteq K \subseteq L$ estensioni. Allora $F \subseteq L$ algebrica $\iff$ $F \subseteq K$ e $K \subseteq L$ algebriche.*

## Dimostrazione.

$\implies$ Chiaro.

$\impliedby$ $\beta \in L \implies \beta$ algebrico su $K \implies \exists\, \alpha_0, \ldots, \alpha_n \in K$ non tutti nulli tali che $\sum_{i=0}^{n} \alpha_i \beta^i = 0 \implies \beta$ algebrico su $F' := F(\alpha_0, \ldots, \alpha_n)$; $\alpha_0, \ldots, \alpha_n$ algebrici su $F \implies$ per la Proposizione precedente $F \subseteq F'$ e $F' \subseteq F'(\beta)$ finite $\implies$ $F \subseteq F'(\beta)$ finita $\implies$ $F \subseteq F(\beta)$ finita $\implies \beta$ algebrico su $F$.

# Chiusura algebrica in un'estensione

## Definizione-Proposizione

*$K \subseteq L$ estensione $\implies$ $\overline{K}^L := \{\alpha \in L : \alpha$ algebrico su $K\}$ è un sottocampo di $L$, detto chiusura algebrica di $K$ in $L$.*
*Inoltre l'estensione $K \subseteq \overline{K}^L$ è algebrica e $\overline{\overline{K}^L}^L = \overline{K}^L$.*

## Dimostrazione.

Chiaramente $K \subseteq \overline{K}^L$ (in particolare $1 \in \overline{K}^L$).
$\alpha, \beta \in \overline{K}^L \implies$ per la Proposizione di prima $K \subseteq K(\alpha, \beta)$ è un'estensione algebrica $\implies$ $\alpha - \beta, \alpha\beta \in K(\alpha, \beta)$ sono algebrici su $K \implies \alpha - \beta, \alpha\beta \in \overline{K}^L$.
Analogamente $0 \neq \alpha \in \overline{K}^L \implies K \subseteq K(\alpha)$ estensione algebrica $\implies \alpha^{-1} \in K(\alpha)$ algebrico su $K \implies \alpha^{-1} \in \overline{K}^L$.
Per definizione l'estensione $K \subseteq \overline{K}^L$ è algebrica. Analogamente è algebrica l'estensione $\overline{K}^L \subseteq \overline{\overline{K}^L}^L$, e quindi anche $K \subseteq \overline{\overline{K}^L}^L$ per la Proposizione precedente. Allora $\overline{\overline{K}^L}^L \subseteq \overline{K}^L$, per cui $\overline{\overline{K}^L}^L = \overline{K}^L$. □

# Chiusura algebrica di un campo

## Definizione

Una chiusura algebrica di un campo $K$ è un'estensione algebrica $K \subseteq \overline{K}$ con $\overline{K}$ algebricamente chiuso.

## Corollario

*$K \subseteq L$ estensione con $L$ algebricamente chiuso $\implies$ $K \subseteq \overline{K}^L$ è una chiusura algebrica di $K$.*

## Dimostrazione.

$K \subseteq \overline{K}^L$ estensione algebrica per la Definizione-Proposizione.
$\overline{K}^L$ algebricamente chiuso: $f \in \overline{K}^L[X] \setminus \overline{K}^L \subseteq L[X] \setminus L \implies$
$\exists\, \alpha \in L$ tale che $f(\alpha) = 0$ (perché $L$ algebricamente chiuso) $\implies$
$\alpha$ algebrico su $\overline{K}^L \implies \alpha \in \overline{\overline{K}^L}^L = \overline{K}^L$. □

## Esempio

$\mathbb{Q} \subseteq \overline{\mathbb{Q}} := \overline{\mathbb{Q}}^{\mathbb{C}}$ è una chiusura algebrica di $\mathbb{Q}$. Si dice che $\alpha \in \mathbb{C}$ è algebrico (risp. trascendente) se $\alpha \in \overline{\mathbb{Q}}$ (risp. $\alpha \notin \overline{\mathbb{Q}}$).

# Esercizio sulle estensioni di $\mathbb{Q}$

## Osservazione

$K \subseteq L$ estensione, $\alpha \in L$, $f \in K[X]$ monico e irriducibile, $f(\alpha) = 0$ $\implies$ $f = \mathrm{m}_{\alpha,K}$ ($\mathrm{m}_{\alpha,K} \mid f$ e sono entrambi monici e irriducibili).

1. $\forall\, n > 0\ \exists\, \alpha \in \mathbb{C}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
2. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.
3. $[\mathbb{R} : \mathbb{Q}] = [\mathbb{C} : \mathbb{Q}] = \infty$.
4. L'estensione $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ non è finitamente generata.

1. $\alpha := \sqrt[n]{2} \in \mathbb{R}$ è radice di $X^n - 2 \in \mathbb{Q}[X]$ monico e irriducibile (per il criterio di Eisenstein relativo al primo 2) $\implies$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(X^n - 2) = n$.
2. $\forall\, n > 0$, dato $\alpha$ come nel punto 1, $\alpha \in \overline{\mathbb{Q}}^{\mathbb{C}} = \overline{\mathbb{Q}}$ $\implies$ $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \overline{\mathbb{Q}}$ estensioni $\implies$ $[\overline{Q} : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
3. $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ estensioni $\implies$ $[\mathbb{C} : \mathbb{Q}] \geq [\overline{Q} : \mathbb{Q}] = \infty$.
   $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ estensioni, $[\mathbb{C} : \mathbb{R}] = 2$, per assurdo $[\mathbb{R} : \mathbb{Q}] = n < \infty$ $\implies$ $[\mathbb{C} : \mathbb{Q}] = 2n < \infty$, assurdo.
4. È algebrica ma non finita (per il punto 2).

# Esercizio sulle estensioni finite

$K \subseteq K' \subseteq L$ estensioni, $\alpha \in L$ con $[K' : K] = n$ e $[K(\alpha) : K] = m$.

1. $\mathrm{mcm}(m, n) \mid [K'(\alpha) : K] \leq mn$ (dunque $[K'(\alpha) : K] = mn$ se $\mathrm{mcd}(m, n) = 1$).
2. $[K'(\alpha) : K] \nmid mn$ se $K = \mathbb{Q}$, $L = \mathbb{C}$, $K' = \mathbb{Q}(\beta)$ con $\alpha$ e $\beta$ radici distinte di $X^3 - 2$.

1. $m' := [K'(\alpha) : K'] \leq m$, $K \subseteq K' \subseteq K'(\alpha)$ estensioni $\implies$ $l := [K'(\alpha) : K] = [K'(\alpha) : K'][K' : K] = m'n \leq mn$.
   $K \subseteq K(\alpha) \subseteq K'(\alpha)$ estensioni $\implies$ $m \mid l$; $n \mid l = m'n$ $\implies$ $\mathrm{mcm}(m, n) \mid l$.
2. $\mathrm{m}_\alpha = \mathrm{m}_\beta = X^3 - 2$ (perché monico e irriducibile in $\mathbb{Q}[X]$) $\implies$ $m = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_\alpha) = 3$ e analogamente $n = 3$.
   $\omega := \alpha\beta^{-1} \in \mathbb{C}$ tale che $K'(\alpha) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta, \omega)$.
   $\omega^3 = \alpha^3\beta^{-3} = 1$ $\implies$ $\omega$ radice di $X^3 - 1 = (X - 1)f$ con $f := (X^2 + X + 1)$ monico e irriducibile in $\mathbb{Q}[X]$; $\omega \neq 1$ $\implies$ $\omega$ radice di $f$ $\implies$ $\mathrm{m}_\omega = f$ $\implies$ $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\mathrm{m}_\omega) = 2$.
   $[K'(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta, \omega) : \mathbb{Q}] = 3 \cdot 2 = 6 \nmid mn = 9$.

# Esercizio

1. $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.
2. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
3. $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Determinare $\mathrm{m}_{\sqrt{2}+\sqrt{3},\mathbb{Q}}$.

1. $\mathrm{m}_{\sqrt{2}} = X^2 - 2 \implies [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathrm{m}_i = X^2 + 1 \implies [\mathbb{Q}(i) : \mathbb{Q}] = 2$. Dunque $l := [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$ tale che $2 = \mathrm{mcm}(2, 2) \mid l \mid 2 \cdot 2 = 4 \implies l = 2$ o 4. Per assurdo $l = 2 \implies [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 1 \implies \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}) \implies i \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, assurdo.
2. Analogamente al punto 1, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$ o 4. Per assurdo sia $2 \implies \sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Poiché $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2 - 2)$, che ha come $\mathbb{Q}$-base $\{\overline{1}, \overline{X}\}$, $\mathbb{Q}(\sqrt{2})$ ha come $\mathbb{Q}$-base $\{1, \sqrt{2}\} \implies \exists!\, a, b \in \mathbb{Q}$ tali che $\sqrt{3} = a + b\sqrt{2} \implies 3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} \implies a^2 + 2b^2 = 3$ e $2ab = 0 \implies a = 0$ e $2b^2 = 3$ o $b = 0$ e $a^2 = 3$, assurdo.

# Dimostrazione di 3 e 4

3. $\alpha := \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3}) \implies \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$, e per dimostrare che $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$ (e quindi concludere che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3})$) basta verificare che $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\alpha)$.
$\alpha^2 = 5+2\sqrt{6} \in \mathbb{Q}(\alpha) \implies \sqrt{6} = (\alpha^2-5)/2 \in \mathbb{Q}(\alpha) \implies$
$\alpha\sqrt{6} = 2\sqrt{3}+3\sqrt{2} \in \mathbb{Q}(\alpha) \implies$
$2\sqrt{3}+3\sqrt{2}-2\alpha = \sqrt{2} \in \mathbb{Q}(\alpha) \implies \alpha-\sqrt{2} = \sqrt{3} \in \mathbb{Q}(\alpha)$.
4. Come visto nel punto 3, $2\sqrt{6} = \alpha^2-5 \implies$

$$24 = (\alpha^2-5)^2 = \alpha^4-10\alpha^2+25$$

$\implies \alpha^4-10\alpha^2+1 = 0 \implies \alpha$ è radice di $f := X^4-10X^2+1 \in \mathbb{Q}[X] \implies \mathrm{m}_\alpha \mid f$. Per i punti 3 e 2

$$\deg(\mathrm{m}_\alpha) = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4 = \deg(f)$$

$\implies \mathrm{m}_\alpha$ e $f$ sono associati $\implies \mathrm{m}_\alpha = f$ perché sono entrambi monici.

# Radice di un polinomio in un'estensione

Dato $f \in K[X]$ (che posso supporre irriducibile e monico), esiste un'estensione $K \subseteq L$ tale che $f$ abbia una radice $\alpha \in L$?
Se la risposta è sì, $f = \mathrm{m}_{\alpha,K}$; inoltre posso supporre $L = K(\alpha)$, e in questo caso $L \cong K[X]/(f)$.

## Proposizione

*$f \in K[X]$ irriducibile e monico, $\pi\colon K[X] \to L := K[X]/(f)$ proiezione al quoziente, $\alpha := \pi(X) \in L \implies \pi|_K\colon K \to L$ estensione, $L = K(\alpha)$ e $f = \mathrm{m}_{\alpha,K}$ (quindi $f$ ha una radice in $L$).*

## Dimostrazione.

$f$ irriducibile $\implies$ $(f)$ ideale massimale $\implies$ $L$ campo.
$\pi|_K$ estensione perché omomorfismo di anelli con $K$ e $L$ campi.
$\pi$ omomorfismo di $K$ algebre tale che $\pi(X) = \alpha \implies \pi(g) = g(\alpha)$
$\forall\, g \in K[X] \implies L = \{g(\alpha) : g \in K[X]\} = K[\alpha] = K(\alpha)$.
$f$ irriducibile e monico, $f(\alpha) = \pi(f) = 0 \implies f = \mathrm{m}_{\alpha,K}$. □

# Campo di spezzamento di un polinomio

## Definizione

Un campo di spezzamento di $f \in K[X] \setminus \{0\}$ è un'estensione $K \subseteq L$ tale che:

- $f$ si spezza su $L$, cioè $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in L$ tali che $f = c\prod_{i=1}^{n}(X - \alpha_i)$;
- $K \subseteq L' \subseteq L$ estensione tale che $f$ si spezza su $L' \implies L' = L$.

Se $K \subseteq L$ è un campo di spezzamento di $f$, si dice anche che $L$ è un campo di spezzamento di $f$ su $K$.

## Osservazione

$K \subseteq L$ estensione tale che $f = c\prod_{i=1}^{n}(X - \alpha_i) \in K[X]$ si spezza su $L \implies \exists!\, K \subseteq L_0 \subseteq L$ estensione tale che $K \subseteq L_0$ è un campo di spezzamento di $f$; inoltre $L_0 = K(\alpha_1, \ldots, \alpha_n)$.
Infatti $f$ si spezza su $K(\alpha_1, \ldots, \alpha_n)$, e se $K \subseteq L' \subseteq L$ è un'estensione tale che $f$ si spezza su $L'$, allora $\alpha_1, \ldots, \alpha_n \in L'$ (per l'unicità della fattorizzazione in $L[X]$), per cui $K(\alpha_1, \ldots, \alpha_n) \subseteq L'$.

# Esistenza del campo di spezzamento

## Teorema

*$K$ campo, $0 \neq f \in K[X]$.*

1. *Esiste un campo di spezzamento di $f$.*
2. *$n := \deg(f)$, $K \subseteq L$ campo di spezzamento di $f$ $\implies$ $[L : K] \mid n!$. Inoltre $n \mid [L : K]$ se $f$ è irriducibile in $K[X]$.*

## Dimostrazione.

1. Per l'Osservazione basta dimostrare che esiste un'estensione $K \subseteq L$ tale che $f$ si spezza su $L$.
   Per induzione su $n$: se $n = 0$, basta prendere $L = K$.
   Se $n > 0$, allora $\exists\, g \in K[X]$ irriducibile tale che $g \mid f$.
   Per la Proposizione $\exists\, K \subseteq K'$ estensione e $\exists\, \alpha \in K'$ tale che $g(\alpha) = 0 \implies f(\alpha) = 0 \implies f = (X - \alpha) f_1$ con $f_1 \in K'[X]$ e $\deg(f_1) = n - 1$.
   Per induzione $\exists\, K' \subseteq L$ estensione tale che $f_1$ si spezza su $L$ $\implies$ $f$ si spezza su $L$.

# Dimostrazione di 2

Per definizione $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in L$ tali che $f = c\prod_{i=1}^{n}(X - \alpha_i)$, e per l'Osservazione $L = K(\alpha_1, \ldots, \alpha_n)$.
Per induzione su $n$: se $n = 0$, allora $f = c \in K^*$ (non irriducibile in $K[X]$) $\implies$ $L = K$ $\implies$ $[L : K] = 1 \mid n! = 1$.
Se $n > 0$ e $f$ è irriducibile in $K[X]$, allora $\mathrm{m}_{\alpha_1,K} = c^{-1}f$ $\implies$ $[K(\alpha_1) : K] = \deg(\mathrm{m}_{\alpha_1,K}) = n$. Posto $n' := [L : K(\alpha_1)]$, $[L : K] = [L : K(\alpha_1)][K(\alpha_1) : K] = n'n$, per cui $n \mid [L : K]$.
$f = (X - \alpha_1)f_1$ in $K(\alpha_1)[X]$ con $f_1 := c\prod_{i=2}^{n}(X - \alpha_i)$ tale che $K(\alpha_1) \subseteq L$ campo di spezzamento di $f_1$ (perché $f_1$ si spezza su $L$ e $L = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$). Poiché $\deg(f_1) = n - 1$, per induzione $n' = [L : K(\alpha_1)] \mid (n-1)!$ $\implies$ $[L : K] = n'n \mid (n-1)!n = n!$.
Se $n > 0$ e $f = gh$ non è irriducibile in $K[X]$ (con $0 < m := \deg(g) < n$), posso supporre $g = c\prod_{i=1}^{m}(X - \alpha_i)$ e $h = \prod_{i=m+1}^{n}(X - \alpha_i)$ $\implies$ $K' := K(\alpha_1, \ldots, \alpha_m)$ campo di spezzamento di $g$ su $K$ e $L$ campo di spezzamento di $h$ su $K'$.
Per induzione $[K' : K] \mid m!$ e $[L : K'] \mid (n-m)!$ $\implies$ $[L : K] = [L : K'][K' : K] \mid (n-m)!m! \mid n!$.

# Esistenza della chiusura algebrica

**Lemma**

*$K$ campo $\implies \exists\, K \to K'$ estensione tale che ogni polinomio non costante a coefficienti in $K$ ha una radice in $K'$.*

**Teorema**

*Ogni campo $K$ ha una chiusura algebrica $K \subseteq \overline{K}$.*

**Dimostrazione.**

- Posto $K_0 := K$, per il Lemma induttivamente $\forall\, n \in \mathbb{N}$ $\exists\, K_n \subseteq K_{n+1}$ estensione tale che $f \in K_n[X] \setminus K \implies f$ ha una radice in $K_{n+1}$.
- $L := \bigcup_{n\in\mathbb{N}} K_n$ campo (esercizio) tale che $K \subseteq L$ estensione con $L$ algebricamente chiuso: $f \in L[X] \setminus L \implies \exists\, n \in \mathbb{N}$ tale che $f \in K_n[X] \implies f$ ha una radice in $K_{n+1} \subseteq L$.
- $\overline{K} := \overline{K}^L$ tale che $K \subseteq \overline{K}$ chiusura algebrica di $K$ (già visto).

# Dimostrazione del Lemma

$U := \{f \in K[X] : f \text{ irriducibile e monico}\}$, $A := K[X_f : f \in U]$.
$I := (f(X_f) : f \in U) \subsetneq A$ ideale: per assurdo $I = A \implies$
$\exists\, f_1, \dots, f_n \in U$ distinti e $g_1, \dots, g_n \in A$ tali che

$$h := \sum_{l=1}^{n} f_i(X_{f_i}) g_i = 1.$$

$K \subseteq L$ campo di spezzamento di $\prod_{i=1}^{n} f_i \implies \forall\, i = 1, \dots, n$
$\exists\, \alpha_i \in L$ tale che $f_i(\alpha_i) = 0$. Valutando $h = 1$ in

$$X_f = \begin{cases} \alpha_i & \text{se } f = f_i \text{ per qualche } i = 1, \dots, n \\ 0 & \text{altrimenti} \end{cases}$$

si ottiene $0 = 1$ in $L$, assurdo.

$\exists\, J \subset A$ ideale massimale tale che $I \subseteq J \implies K' := A/J$ campo e $\pi|_K \colon K \to K'$ (con $\pi \colon A \to K'$ proiezione) estensione di campi con la proprietà richiesta: dato $f \in K[X] \setminus K$, posso supporre $f \in U$ $\implies f(\pi(X_f)) = \pi(f(X_f)) = 0$ perché $f(X_f) \in I \subseteq J = \ker(\pi)$.

# Omomorfismi e isomorfismi di estensioni

## Definizione

$i\colon K \to L$ e $i'\colon K \to L'$ estensioni. Un omomorfismo di estensioni di $K$ (o semplicemente un $K$-omomorfismo) da $i$ a $i'$ è un omomorfismo di $K$-algebre, cioè un omomorfismo di anelli $j\colon L \to L'$ tale che $i' = j \circ i$.
Un tale omomorfismo è un isomorfismo di estensioni di $K$ (o semplicemente un $K$-isomorfismo) se $j$ è un isomorfismo.

## Osservazione

$i\colon K \to L$ estensione induce omomorfismo di anelli

$$i\colon K[X] \to L[X] \qquad f = \sum_{n\geq 0} a_n X^n \mapsto i(f) = \sum_{n\geq 0} i(a_n) X^n.$$

Spesso si scriverà ancora $f$ invece di $i(f) \in L[X]$. Se $\alpha \in L$, l'identificazione tra $f(\alpha) = \sum_{n\geq 0} a_n \alpha^n$ e $i(f)(\alpha) = \sum_{n\geq 0} i(a_n)\alpha^n$ è coerente con la struttura di $K$-spazio vettoriale su $L$.

# Esistenza di omomorfismi di estensioni

## Proposizione

*$K \subseteq K'$ e $i\colon K \to L$ estensioni, $\alpha \in K'$ algebrico su $K$, $\beta \in L$. Allora esiste un $K$-omomorfismo $j\colon K(\alpha) \to L$ tale che $j(\alpha) = \beta$ $\iff$ $\mathrm{m}_{\alpha,K}(\beta) = 0$; inoltre se esiste è unico.*

## Dimostrazione.

$\alpha$ algebrico su $K$ $\implies$ $K(\alpha) = K[\alpha] \cong K[X]/(\mathrm{m}_{\alpha,K})$.

Dunque va dimostrato che $\exists$ (unico) $K$-omomorfismo $K[X]/(\mathrm{m}_{\alpha,K}) \to L$ tale che $\overline{X} \mapsto \beta$ $\iff$ $\mathrm{m}_{\alpha,K}(\beta) = 0$.

Per il teorema di omomorfismo per anelli dare un omomorfismo di anelli $\overline{\varphi}\colon K[X]/(\mathrm{m}_{\alpha,K}) \to L$ equivale a dare un omomorfismo di anelli $\varphi\colon K[X] \to L$ tale che $(\mathrm{m}_{\alpha,K}) \subseteq \ker(\varphi)$, e chiaramente $\overline{\varphi}$ è un $K$-omomorfismo $\iff$ $\varphi$ è un omomorfismo di $K$-algebre.

Poiché $\forall\, \beta \in L\ \exists!\, \varphi\colon K[X] \to L$ omomorfismo di $K$-algebre tale che $\varphi(X) = \beta$, per concludere basta osservare che per un tale $\varphi$ $(\mathrm{m}_{\alpha,K}) \subseteq \ker(\varphi)$ $\iff$ $0 = \varphi(\mathrm{m}_{\alpha,K}) = \mathrm{m}_{\alpha,K}(\beta)$. □

# Unicità del campo di spezzamento

## Teorema

*$K \subseteq K'$ campo di spezzamento di $f \in K[X] \setminus \{0\}$, $i\colon K \to L$ estensione. Allora esiste un $K$-omomorfismo $i'\colon K' \to L \iff f$ si spezza su $L$.*

## Corollario

*$K$ campo, $f \in K[X] \setminus \{0\} \implies$ un campo di spezzamento di $f$ esiste e è unico a meno di $K$-isomorfismo.*

## Dimostrazione.

Esistenza già vista.

Se $K \subseteq K'$ e $i\colon K \to L$ sono due campi di spezzamento di $f$, per il Teorema $\exists$ $K$-omomorfismo $i'\colon K' \to L$. Sempre per il Teorema $f$ si spezza su $i'(K') \subseteq L \implies i'(K') = L$. $\square$

## Osservazione

Segue dal Corollario che il grado $[K' : K]$ di un campo di spezzamento $K \subseteq K'$ di $f \in K[X] \setminus \{0\}$ dipende solo da $f$.

# Dimostrazione del Teorema

Per ipotesi $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in K'$ (con $n = \deg(f)$) tali che $f = c\prod_{l=1}^{n}(X - \alpha_l)$ e $K' = K(\alpha_1, \ldots, \alpha_n)$.

$\Longrightarrow$ $f = i'(f) = c\prod_{l=1}^{n}(X - i'(\alpha_l))$ si spezza su $L$.

$\Longleftarrow$ Per induzione su $n$: $n = 0 \implies K' = K$ e $i' = i$.
$n > 0 \implies \mathrm{m}_{\alpha_1,K}$ si spezza su $L$ (perché $\mathrm{m}_{\alpha_1,K} \mid f$ e $f$ si spezza su $L$) $\implies \exists\, \beta \in L$ tale che $\mathrm{m}_{\alpha_1,K}(\beta) = 0 \implies$ per la Proposizione $\exists$ $K$-omomorfismo $j\colon K(\alpha_1) \to L$ (tale che $j(\alpha_1) = \beta$) $\implies$

$$g := \prod_{l=2}^{n}(X - \alpha_l) \in K(\alpha_1)[X]$$

tale che $\deg(g) = n - 1$, $K(\alpha_1) \subseteq K'$ campo di spezzamento di $g$ e $g$ si spezza su $L$ (perché $g \mid f$ e $f$ si spezza su $L$) $\implies$ per induzione $\exists$ $K(\alpha_1)$-omomorfismo (e dunque $K$-omomorfismo) $i'\colon K' \to L$.

# Unicità della chiusura algebrica

## Teorema

*$K \subseteq L$ estensione algebrica, $i\colon K \to \overline{K}$ chiusura algebrica di $K$*
$\implies$ *esiste un $K$-omomorfismo $j\colon L \to \overline{K}$.*

## Osservazione

$L \subseteq L'$ estensione algebrica, $L$ algebricamente chiuso $\implies$ $L = L'$:
$\alpha \in L' \implies \mathrm{m}_{\alpha,L} \in L[X]$ irriducibile e monico con una radice in $L$
$\implies \deg(\mathrm{m}_{\alpha,L}) = 1 \implies \mathrm{m}_{\alpha,L} = X - \alpha \implies \alpha \in L$.

## Corollario

*$K$ campo $\implies$ una chiusura algebrica di $K$ è unica a meno di $K$-isomorfismo.*

## Dimostrazione.

$K \subseteq L$ e $i\colon K \to \overline{K}$ chiusure algebriche di $K$ $\implies$ per il Teorema
$\exists$ $K$-omomorfismo $j\colon L \to \overline{K}$.
$j$ estensione algebrica (perché $i$ lo è), $L$ algebricamente chiuso
$\implies$ $j$ $K$-isomorfismo per l'Osservazione.

# Dimostrazione del Teorema

Nell'insieme parzialmente ordinato e $\neq \emptyset$

$$\{(L', j') : K \subseteq L' \subseteq L \text{ estensioni, } j' : L' \to \overline{K} \ K\text{-omomorifsmo}\}$$

(in cui $(L', j') \leq (L'', j'') \iff L' \subseteq L''$ e $j''|_{L'} = j'$) ogni catena $\{(L_\lambda, j_\lambda) : \lambda \in \Lambda\}$ ha un maggiorante $(\tilde{L}, \tilde{j})$ con $\tilde{L} := \bigcup_{\lambda \in \Lambda} L_\lambda$ e

$$\tilde{j} : \tilde{L} \to \overline{K} \qquad \alpha \mapsto j_\lambda(\alpha) \qquad \text{se } \alpha \in L_\lambda$$

(esercizio). Per il lemma di Zorn esiste un elemento massimale $(L_0, j_0)$, e basta dimostrare $L_0 = L$.
$\alpha \in L \implies \alpha$ algebrico su $K \implies \alpha$ algebrico su $L_0$.
$\overline{K}$ algebricamente chiuso $\implies \exists\, \beta \in \overline{K}$ tale che $\mathrm{m}_{\alpha, L_0}(\beta) = 0$
$\implies$ per la Proposizione $\exists$ $L_0$-omomorfismo $j_0' : L_0(\alpha) \to \overline{K}$ (tale che $j_0'(\alpha) = \beta$) $\implies (L_0, j_0) \leq (L_0(\alpha), j_0') \implies L_0 = L_0(\alpha)$ per la massimalità di $(L_0, j_0) \implies \alpha \in L_0$.

# Estensioni normali

## Definizione

Un'estensione algebrica $K \subseteq L$ è normale se $\mathrm{m}_{\alpha,K}$ si spezza su $L$ $\forall\, \alpha \in L$.

## Esempio

$K \subseteq \overline{K}$ chiusura algebrica di $K \implies K \subseteq \overline{K}$ è normale.

## Proposizione

*Un'estensione finita $K \subseteq L$ è normale $\iff$ è campo di spezzamento di un polinomio.*

## Dimostrazione di $\implies$.

$\exists\, \alpha_1, \ldots, \alpha_n \in L$ algebrici su $K$ tali che $L = K(\alpha_1, \ldots, \alpha_n) \implies$ $K \subseteq L$ campo di spezzamento di $f := \prod_{l=1}^{n} \mathrm{m}_{\alpha_l,K}$:
$f$ si spezza su $L$ perché $\mathrm{m}_{\alpha_1,K}, \ldots, \mathrm{m}_{\alpha_n,K}$ per ipotesi si spezzano su $L$ e $L = K(U)$ con $U := \{\alpha \in L : f(\alpha) = 0\}$, dato che $\alpha_1, \ldots, \alpha_n \in U$ e $L = K(\alpha_1, \ldots, \alpha_n)$.

# Dimostrazione di $\Longleftarrow$

- $K \subseteq L$ campo di spezzamento di $f \in K[X] \setminus \{0\} \implies$ $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in L$ tali che $f = c\prod_{l=1}^{n}(X - \alpha_l)$ e $L = K(\alpha_1, \ldots, \alpha_n)$.
- $\alpha \in L \implies \exists\, L \subseteq L'$ campo di spezzamento di $\mathrm{m}_{\alpha,K}$. Dato $\beta \in L'$ tale che $\mathrm{m}_{\alpha,K}(\beta) = 0$, devo dimostrare $\beta \in L$.
- $\exists!$ $K$-omomorfismo $i\colon K(\alpha) \to L'$ tale che $i(\alpha) = \beta$.
- $K(\alpha) \subseteq L$ campo di spezzamento di $f$, $f = i(f)$ si spezza su $L' \implies \exists$ $K(\alpha)$-omomorfismo $j\colon L \to L'$ (cioè tale che $j|_{K(\alpha)} = i$).
- $j$ $K$-omomorfismo $\implies \forall\, l = 1, \ldots, n$

$$f(j(\alpha_l)) = j(f)(j(\alpha_l)) = j(f(\alpha_l)) = j(0) = 0$$

$\implies j(\alpha_l) \in \{\alpha_1, \ldots, \alpha_n\} \subseteq L \implies j(L) \subseteq L \implies$ $\beta = i(\alpha) = j(\alpha) \in j(L) \subseteq L$.

# Proprietà delle estensioni normali

$F \subseteq K \subseteq L$ estensioni.

- $F \subseteq L$ normale $\implies$ $K \subseteq L$ normale: $\alpha \in L \implies \mathrm{m}_{\alpha,K}$ si spezza su $L$ perché $\mathrm{m}_{\alpha,K} \mid \mathrm{m}_{\alpha,F}$ e $\mathrm{m}_{\alpha,F}$ si spezza su $L$.
- $F \subseteq L$ finita e normale $\not\implies$ $F \subseteq K$ normale: per esempio, $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ e $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ con $\omega^3 = 1$ e $\omega \neq 1$ ($F \subseteq K$ non normale perché $\mathrm{m}_{\sqrt[3]{2},F} = X^3 - 2$ non si spezza su $K \subseteq \mathbb{R}$, $F \subseteq L$ normale perché campo di spezzamento di $X^3 - 2$).
- $[L : K] = 2 \implies K \subseteq L$ normale: $\alpha \in L \setminus K \implies L = K(\alpha)$ $\implies \deg(\mathrm{m}_{\alpha,K}) = [K(\alpha) : K] = 2 \implies K \subseteq L$ campo di spezzamento di $\mathrm{m}_{\alpha,K}$.
- $F \subseteq K$ e $K \subseteq L$ finite e normali $\not\implies$ $F \subseteq L$ normale: per esempio, $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$ e $L = \mathbb{Q}(\sqrt[4]{2})$ ($F \subseteq K$ e $K \subseteq L$ normali perché di grado 2, $F \subseteq L$ non normale perché $\mathrm{m}_{\sqrt[4]{2},F} = X^4 - 2$ non si spezza su $L \subseteq \mathbb{R}$).

# Gruppo di Galois di un'estensione

Il gruppo degli automorfismi di un campo $K$ è

$$\mathrm{G}(K) := \{\sigma \colon K \to K \ : \ \sigma \text{ isomorfismo di anelli}\} < S(K).$$

## Definizione

Il gruppo di Galois di un'estensione $F \subseteq K$ è

$$\mathrm{G}_F(K) := \{\sigma \in \mathrm{G}(K) \ : \ \sigma(a) = a \ \forall\, a \in F\} < \mathrm{G}(K).$$

## Proposizione

*$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ finita e normale.*
*Allora $F \subseteq K$ è normale $\iff$ $K$ è $\mathrm{G}_F(L)$-stabile (cioè $\sigma(K) = K$ $\forall\, \sigma \in \mathrm{G}_F(L)$, o, equivalentemente, $\sigma(K) \subseteq K$ $\forall\, \sigma \in \mathrm{G}_F(L)$).*

# Dimostrazione della Proposizione

$\Longrightarrow$ $\sigma \in \mathrm{G}_F(L) \implies \sigma(K) \subseteq K$:

$\alpha \in K \implies \mathrm{m}_{\alpha,F}(\sigma(\alpha)) = \sigma(\mathrm{m}_{\alpha,F}(\alpha)) = \sigma(0) = 0 \implies$ $\sigma(\alpha) \in K$ perché $\mathrm{m}_{\alpha,F}$ si spezza su $K$.

$\Longleftarrow$ $F \subseteq L$ normale e finita $\implies$ $F \subseteq L$ campo di spezzamento di $f \in F[X] \setminus \{0\}$.

$\alpha \in K \implies \mathrm{m}_{\alpha,F}$ si spezza su $L$, e va dimostrato che si spezza su $K$, cioè che $\beta \in L$ tale che $\mathrm{m}_{\alpha,F}(\beta) = 0 \implies$ $\beta \in K$.

$\exists!$ $F$-omomorfismo $i\colon F(\alpha) \to L$ tale che $i(\alpha) = \beta$.
$F(\alpha) \subseteq L$ campo di spezzamento di $f$, $f = i(f)$ si spezza su $L$ $\implies$ $\exists$ $F(\alpha)$-omomorfismo (e quindi $F$-omomorfismo) $\sigma\colon L \to L$ (cioè tale che $\sigma|_{F(\alpha)} = i$).

$\sigma(L) \subseteq L$, $\dim_F(\sigma(L)) = \dim_F(L) < \infty \implies \sigma(L) = L \implies$ $\sigma \in \mathrm{G}_F(L) \implies \beta = i(\alpha) = \sigma(\alpha) \in \sigma(K) = K$.

# Polinomi separabili

## Definizione

$K$ campo. $f \in K[X]$ irriducibile è separabile (su $K$) se ha $\deg(f)$ radici distinte in un campo di spezzamento.

Ricordiamo che, se $K \subseteq L$ è un'estensione, $f \in K[X]$ e $\alpha \in L$ è radice di $f$ (cioè $(X-\alpha) \mid f$), allora $\alpha$ è radice multipla di $f$ (cioè $(X-\alpha)^2 \mid f$) $\iff$ $\alpha$ è radice della derivata $f'$ di $f$.

## Lemma

*$f \in K[X]$ irriducibile è separabile* $\iff$ $f' \neq 0$.

## Dimostrazione.

$K \subseteq L$ campo di spezzamento di $f$.

$\implies$ $\exists\, \alpha \in L$ radice non multipla di $f$ $\implies$ $f'(\alpha) \neq 0$ $\implies$ $f' \neq 0$.

$\impliedby$ $\deg(f') < \deg(f)$ $\implies$ $f \nmid f'$ $\implies$ $\mathrm{mcd}(f, f') = 1$ in $K[X]$ (perché $f$ irriducibile in $K[X]$) $\implies$ $\exists\, g, h \in K[X]$ tali che $1 = gf + hf'$ $\implies$ $\mathrm{mcd}(f, f') = 1$ in $L[X]$ $\implies$ $f$ non ha radici multiple in $L$, cioè $f$ è separabile.

# Omomorfismo di Frobenius

## Corollario

$\mathrm{char}(K) = 0$, $f \in K[X]$ *irriducibile* $\implies$ $f$ *separabile.*

## Dimostrazione.

$f$ irriducibile $\implies$ $n := \deg(f) > 0$; $f = \sum_{i=0}^{n} a_i X^i$ con $a_n \neq 0$ $\implies$ $f' = \sum_{i=1}^{n} i a_i X^{i-1} \neq 0$ (e $\deg(f') = n - 1$) perché $n a_n \neq 0$ in $K$ $\implies$ $f$ separabile per il Lemma. □

## Definizione-Proposizione

*$A$ dominio, $\mathrm{char}(A) = p$ primo. L'omomorfismo di Frobenius (di $A$) è l'omomorfismo di anelli $\mathcal{F} : A \to A$, $a \mapsto a^p$.*

## Dimostrazione.

$\mathcal{F}(1) = 1$; $\forall\, a, b \in A$ $\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b)$ e

$\mathcal{F}(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p = \mathcal{F}(a) + \mathcal{F}(b)$

perché $p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$ per $0 < i < p$. □

# Campi perfetti

## Definizione

Un campo $K$ è perfetto se $\mathrm{char}(K) = 0$ o $\mathrm{char}(K) = p$ primo e $\mathcal{F}\colon K \to K$ è suriettivo (nel qual caso $\mathcal{F} \in \mathrm{G}(K)$).

## Proposizione

*$K$ campo è perfetto $\iff$ $f$ è separabile $\forall\, f \in K[X]$ irriducibile.*

## Dimostrazione.

Posso supporre $\mathrm{char}(K) = p$ primo.

$\Longrightarrow$ $f \in K[X]$ irriducibile $\Longrightarrow$ per il Lemma basta dimostrare $f' \neq 0$. Per assurdo $f' = 0 \implies f = \sum_{i=0}^{n} a_i X^{pi}$; $K$ perfetto $\implies \exists\, b_i \in K$ tale che $a_i = \mathcal{F}(b_i) = b_i^p \ \forall\, i = 0, \dots, n \implies f = \mathcal{F}(\sum_{i=0}^{n} b_i X^i) = (\sum_{i=0}^{n} b_i X^i)^p$, assurdo.

$\Longleftarrow$ $a \in K \implies \exists\, K \subseteq L$ estensione tale che $X^p - a$ ha una radice $\alpha$ in $L \implies \mathrm{m}_{\alpha,K} \mid (X^p - a) = X^p - \alpha^p = (X - \alpha)^p \implies \mathrm{m}_{\alpha,K} = X - \alpha$ (perché $\mathrm{m}_{\alpha,K}$ monico e irriducibile, quindi separabile) $\implies \alpha \in K$ e $a = \alpha^p = \mathcal{F}(\alpha)$.

# Estensioni separabili

## Definizione

$K \subseteq L$ estensione.

- $\alpha \in L$ è separabile su $K$ se $\alpha$ è algebrico su $K$ e $\mathrm{m}_{\alpha,K}$ è separabile.
- $K \subseteq L$ è separabile se $\alpha$ è separabile su $K$ $\forall\, \alpha \in L$.

## Osservazione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ separabile $\implies$ $F \subseteq K$ separabile (ovvio) e $K \subseteq L$ separabile (perché $\mathrm{m}_{\alpha,K} \mid \mathrm{m}_{\alpha,F}$ $\forall\, \alpha \in L$).

## Corollario

*$K$ è perfetto $\iff$ ogni estensione algebrica di $K$ è separabile.*

## Dimostrazione.

Segue dalla Proposizione precedente, tenendo conto che $f \in K[X]$ irriducibile e monico $\implies$ $\exists\, K \subseteq L$ estensione algebrica e $\exists\, \alpha \in L$ tale che $f = \mathrm{m}_{\alpha,K}$.

# Esempi di campi perfetti

- $K$ finito $\implies$ $K$ perfetto:
  $\mathrm{char}(K) = p$ primo e $\mathcal{F}\colon K \to K$ è suriettivo perché iniettivo.
- $K$ algebricamente chiuso $\implies$ $K$ perfetto:
  posso supporre $\mathrm{char}(K) = p$ primo $\implies$ $\mathcal{F}\colon K \to K$ è suriettivo perché $\forall\, a \in K$ $X^p - a$ ha una radice $b \in K$, cioè $a = b^p = \mathcal{F}(b)$.
- $K \subseteq L$ estensione algebrica, $K$ perfetto $\implies$ $L$ perfetto:
  per il Corollario basta dimostrare ogni estensione algebrica $L \subseteq L'$ è separabile.
  $K \subseteq L$ e $L \subseteq L'$ algebriche $\implies$ $K \subseteq L'$ algebrica $\implies$ $K \subseteq L'$ separabile (sempre per il Corollario) $\implies$ $L \subseteq L'$ separabile.
- $\mathrm{char}(K) = p$ primo $\implies$ $K(X)$ non perfetto:
  per assurdo $\exists\, f/g \in K(X)$ (con $f, g \in K[X]$ e $g \neq 0$) tale che $X = \mathcal{F}(f/g) = f^p/g^p$ $\implies$ $f^p = Xg^p$ in $K[X]$, assurdo.

# $K$-omomorfismi da un'estensione finita

**Teorema**

*$K \subseteq L$ e $i\colon K \to L'$ estensioni con $[L : K] < \infty \implies$*

$$\#\{j\colon L \to L' \ :\ j \ K\text{-omomorfismo}\} \leq [L : K]$$

*e vale l'uguaglianza $\iff$ $\mathrm{m}_{\alpha,K}$ ha $\deg(\mathrm{m}_{\alpha,K})$ radici distinte in $L'$ (cioè $\mathrm{m}_{\alpha,K}$ è separabile e si spezza su $L'$) $\forall\, \alpha \in L$.*

**Dimostrazione (inizio).**

Date estensioni $K \subseteq K' \subseteq K'' \subseteq L$ e un $K$-omomorfismo $i'\colon K' \to L'$, posto

$$E(K'', i') := \{i''\colon K'' \to L' \ :\ i'' \text{ omomorfismo di anelli, } i''|_{K'} = i'\},$$

la disuguaglianza da dimostrare è $\#E(L, i) \leq n := [L : K]$.
Per induzione su $n$: chiaro per $n = 1$, quindi assumiamo $n > 1$.

# Dimostrazione (fine)

$\forall\, \alpha \in L$ sappiamo che $e_\alpha := \#E(K(\alpha), i)$ soddisfa

$$e_\alpha = \#\{\alpha' \in L' \,:\, \mathrm{m}_{\alpha,K}(\alpha') = 0\} \leq \deg(\mathrm{m}_{\alpha,K}) = [K(\alpha) : K] =: n_\alpha$$

e che $e_\alpha = n_\alpha \iff \mathrm{m}_{\alpha,K}$ ha $n_\alpha$ radici distinte in $L'$.
$\alpha \notin K \implies n_\alpha > 1 \implies [L : K(\alpha)] = n/n_\alpha < n \implies$
$\forall\, i' \in E(K(\alpha), i)$ per induzione $\#E(L, i') \leq n/n_\alpha$ e vale l'uguale
$\iff \mathrm{m}_{\beta,K(\alpha)}$ ha $\deg(\mathrm{m}_{\beta,K(\alpha)})$ radici distinte in $L'$ $\forall\, \beta \in L$.
Da $E(L, i) = \coprod_{i' \in E(K(\alpha), i)} E(L, i')$ segue

$$\#E(L, i) = \sum_{i' \in E(K(\alpha), i)} \#E(L, i') \leq e_\alpha n/n_\alpha \leq n_\alpha n/n_\alpha = n$$

e se vale l'uguale allora $e_\alpha = n_\alpha$, per cui $\mathrm{m}_{\alpha,K}$ ha $n_\alpha = \deg(\mathrm{m}_{\alpha,K})$ radici distinte in $L'$ ($\forall\, \alpha \in L \setminus K$, ma ovviamente anche $\forall\, \alpha \in K$).
Viceversa, se $\mathrm{m}_{\alpha,K}$ ha $\deg(\mathrm{m}_{\alpha,K})$ radici distinte in $L'$ $\forall\, \alpha \in L$, fissato $\alpha \in L \setminus K$ si ha $e_\alpha = n_\alpha$ e $\#E(L, i') = n/n_\alpha$
$\forall\, i' \in E(K(\alpha), i)$ (perché $\mathrm{m}_{\beta,K(\alpha)}$ ha $\deg(\mathrm{m}_{\beta,K(\alpha)})$ radici distinte in $L'$ $\forall\, \beta \in L$, dato che $\mathrm{m}_{\beta,K(\alpha)} \mid \mathrm{m}_{\beta,K}$), e quindi $\#E(L, i) = n$.

# Estensioni di Galois

## Definizione

Un'estensione è di Galois se è finita, normale e separabile.

## Osservazione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ di Galois $\implies$ $K \subseteq L$ di Galois.

## Corollario

*$K \subseteq L$ estensione finita* $\implies$ $\#\mathrm{G}_K(L) \leq [L : K]$ *e vale l'uguaglianza* $\iff$ *$K \subseteq L$ è di Galois.*

## Dimostrazione.

$j \colon L \to L$ $K$-omomorfismo $\implies$ $j$ suriettivo (perché $j$ omomorfismo iniettivo di $K$-spazi vettoriali e $\dim_K(L) < \infty$) $\implies$ per il Teorema

$$\#\mathrm{G}_K(L) = \#\{j \colon L \to L \,:\, j \text{ } K\text{-omomorfismo}\} \leq [L : K]$$

e vale l'uguaglianza $\iff$ $\mathrm{m}_{\alpha,K}$ separabile e si spezza su $L$ $\forall\, \alpha \in L$ $\iff$ $K \subseteq L$ separabile e normale $\iff$ $K \subseteq L$ di Galois. $\square$

# Campo fisso di un gruppo di automorfismi

$G$ gruppo, $X$ $G$-insieme $\implies$

$$X^G := \{x \in X \,:\, gx = x \;\forall\, g \in G\} \subseteq X.$$

$L$ campo, $G < \mathrm{G}(L)$ $\implies$

$$L^G = \{\alpha \in L \,:\, \sigma(\alpha) = \alpha \;\forall\, \sigma \in G\} \subseteq L$$

sottocampo (detto campo fisso di $G$).

## Osservazione

$F \subseteq L$ sottocampo primo $\implies$ $F \subseteq L^{\mathrm{G}(L)}$ (perché $L^{\mathrm{G}(L)} \subseteq L$ sottocampo) $\implies$ $\mathrm{G}_F(L) = \mathrm{G}(L)$.

## Teorema (Artin)

*$L$ campo, $G < \mathrm{G}(L)$ finito* $\implies$ $[L : L^G] \leq \#G$.

## Dimostrazione (inizio).

$\#G = m$, $G = \{\sigma_1 = \mathrm{id}_L, \ldots, \sigma_m\}$.
Dati $\alpha_1, \ldots, \alpha_n \in L$ distinti con $n > m$, basta dimostrare che $\{\alpha_1, \ldots, \alpha_n\}$ è linearmente dipendente su $L^G$.

# Dimostrazione (fine)

$v_j := (\sigma_1(\alpha_j), \ldots, \sigma_m(\alpha_j)) \in L^m$ (per $j = 1, \ldots, n$) distinti.
$\{v_1, \ldots, v_n\}$ linearmente dipendente su $L$ (perché $n > m$) $\implies$

$$W := \{(\beta_1, \ldots, \beta_n) \in L^n : \sum_{j=1}^{n} \beta_j v_j = 0\}$$

$L$-sottospazio vettoriale non nullo di $L^n$.
$\sigma \in G$, $(\beta_1, \ldots, \beta_n) \in W \implies (\sigma(\beta_1), \ldots, \sigma(\beta_n)) \in W$:
$(\beta_1, \ldots, \beta_n) \in W \iff \sum_{j=1}^{n} \beta_j \sigma_i(\alpha_j) = 0 \ \forall\, i = 1, \ldots, m \implies$
$\sum_{j=1}^{n} \sigma(\beta_j)(\sigma \circ \sigma_i)(\alpha_j) = 0 \ \forall\, i = 1, \ldots, m \iff$
$(\sigma(\beta_1), \ldots, \sigma(\beta_n)) \in W$ perché $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_m\} = G$.
$(\gamma_1, \ldots, \gamma_n) \in W \setminus \{0\}$ ($\implies \exists j_0 \in \{1, \ldots, n\}$ tale che $\gamma_{j_0} \neq 0$ e posso supporre $\gamma_{j_0} = 1$) con il minimo numero di componenti $\neq 0$.
$\sigma \in G \implies \delta_j := \gamma_j - \sigma(\gamma_j)$ tali che $(\delta_1, \ldots, \delta_n) \in W$ e $\delta_j = 0$ se $\gamma_j = 0$ o $j = j_0 \implies (\delta_1, \ldots, \delta_n) = 0$ per l'ipotesi su $(\gamma_1, \ldots, \gamma_n)$
$\implies \gamma_j = \sigma(\gamma_j) \in L^G$ (per $j = 1, \ldots, n$) tali che $\sum_{j=1}^{n} \gamma_j \alpha_j = 0$ perché $\sum_{j=1}^{n} \gamma_j \sigma_1(\alpha_j) = 0$ e $\sigma_1 = \mathrm{id}_L$.

# Corrispondenza tra sottocampi e sottogruppi

$L$ campo $\implies$ le funzioni

$$\phi\colon \{K : K \subseteq L \text{ sottocampo}\} \to \{G : G < \mathrm{G}(L)\} \quad K \mapsto \mathrm{G}_K(L)$$
$$\psi\colon \{G : G < \mathrm{G}(L)\} \to \{K : K \subseteq L \text{ sottocampo}\} \quad G \mapsto L^G$$

soddifano le seguenti proprietà:

i $K' \subseteq K \subseteq L$ sottocampi $\implies$ $\phi(K) \subseteq \phi(K')$ (cioè $\mathrm{G}_K(L) < \mathrm{G}_{K'}(L)$);

ii $G' < G < \mathrm{G}(L) \implies \psi(G) \subseteq \psi(G')$ (cioè $L^G \subseteq L^{G'}$);

iii $K \subseteq L$ sottocampo $\implies$ $K \subseteq \psi(\phi(K))$ (cioè $K \subseteq L^{\mathrm{G}_K(L)}$);

iv $G < \mathrm{G}(L) \implies G \subseteq \phi(\psi(G))$ (cioè $G < \mathrm{G}_{L^G}(L)$).

Segue formalmente che valgono queste ulteriori proprietà:

v $K \subseteq L$ sottocampo $\implies$ $\phi(K) = \phi(\psi(\phi(K)))$ (cioè $\mathrm{G}_K(L) = \mathrm{G}_{L^{\mathrm{G}_K(L)}}(L)$) perché $\phi(K) \subseteq \phi(\psi(\phi(K)))$ per iv e $K \subseteq \psi(\phi(K))$ per iii, quindi $\phi(\psi(\phi(K))) \subseteq \phi(K)$ per i;

vi $G < \mathrm{G}(L) \implies \psi(G) = \psi(\phi(\psi(G)))$ (cioè $L^G = L^{\mathrm{G}_{L^G}(L)}$).

# Corrispondenza nel caso finito

Da v e vi segue anche che $\phi|_{\mathrm{im}(\psi)}\colon \mathrm{im}(\psi) \to \mathrm{im}(\phi)$ è biunivoca con inversa $\psi|_{\mathrm{im}(\phi)}\colon \mathrm{im}(\phi) \to \mathrm{im}(\psi)$, dove $\mathrm{im}(\psi) = \{L^G : G < \mathrm{G}(L)\}$ e $\mathrm{im}(\phi) = \{\mathrm{G}_K(L) : K \subseteq L \text{ sottocampo}\}$.

## Teorema

1. $G < \mathrm{G}(L)$ *finito* $\implies$ $[L : L^G] = \#G$, $L^G \subseteq L$ *di Galois e* $G = \mathrm{G}_{L^G}(L)$.
2. $K \subseteq L$ *estensione finita* $\implies$ $\#\mathrm{G}_K(L) \leq [L : K]$ *e vale l'uguaglianza* $\iff$ $K \subseteq L$ *di Galois* $\iff$ $K = L^{\mathrm{G}_K(L)}$.

## Corollario

$$\{K : K \subseteq L \text{ di Galois}\} \to \{G : G < \mathrm{G}(L) \text{ finito}\} \quad K \mapsto \mathrm{G}_K(L)$$

$$\{G : G < \mathrm{G}(L) \text{ finito}\} \to \{K : K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

*sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre* $K \subseteq L$ *di Galois* $\implies$ $\#\mathrm{G}_K(L) = [L : K]$.

# Dimostrazione del Teorema

Sappiamo già che:

1' $G < \mathrm{G}(L)$ finito $\implies [L : L^G] \leq \#G$;

2' $K \subseteq L$ estensione finita $\implies \#\mathrm{G}_K(L) \leq [L : K]$ e vale l'uguaglianza $\iff K \subseteq L$ di Galois.

1. Per 1' $[L : L^G] \leq \#G < \infty$.
   Per iv $G < \mathrm{G}_{L^G}(L)$, e quindi $\#G \leq \#\mathrm{G}_{L^G}(L)$.
   Per 2' $\#\mathrm{G}_{L^G}(L) \leq [L : L^G]$.
   Dunque $[L : L^G] = \#G = \#\mathrm{G}_{L^G}(L)$ (per cui $G = \mathrm{G}_{L^G}(L)$) e, ancora per 2', $L^G \subseteq L$ di Galois.
2. Per iii $K \subseteq L^{\mathrm{G}_K(L)}$.
   Per 2' $\#\mathrm{G}_K(L) \leq [L : K] < \infty$.
   Per 1 $L^{\mathrm{G}_K(L)} \subseteq L$ di Galois e $[L : L^{\mathrm{G}_K(L)}] = \#\mathrm{G}_K(L)$.
   Dunque, se $K = L^{\mathrm{G}_K(L)}$, allora $K \subseteq L$ è di Galois.
   Viceversa, se $K \subseteq L$ è di Galois, allora, sempre per 2', $[L : K] = \#\mathrm{G}_K(L) = [L : L^{\mathrm{G}_K(L)}]$, da cui segue $K = L^{\mathrm{G}_K(L)}$.

# Il teorema fondamentale

Ricordiamo che, fissato un campo $L$,

$$\{K : K \subseteq L \text{ di Galois}\} \to \{G : G < \mathrm{G}(L) \text{ finito}\} \quad K \mapsto \mathrm{G}_K(L)$$

$$\{G : G < \mathrm{G}(L) \text{ finito}\} \to \{K : K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre $K \subseteq L$ di Galois $\implies \#\mathrm{G}_K(L) = [L : K]$.

## Teorema fondamentale della teoria di Galois

$K \subseteq L$ estensione di Galois, $G := \mathrm{G}_K(L)$. Allora

$$\{F : K \subseteq F \subseteq L \text{ sottocampo}\} \to \{H : H < G\} \quad F \mapsto \mathrm{G}_F(L)$$

$$\{H : H < G\} \to \{F : K \subseteq F \subseteq L \text{ sottocampo}\} \quad H \mapsto L^H$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre, se $K \subseteq F \subseteq L$ è un sottocampo, allora

1. $F \subseteq L$ di Galois e $\#\mathrm{G}_F(L) = [L : F]$;
2. $K \subseteq F$ normale $\iff H := \mathrm{G}_F(L) \triangleleft G \implies \mathrm{G}_K(F) \cong G/H$.

# Dimostrazione

- La prima parte e il punto 1 seguono da quanto già visto, tenendo conto che $K \subseteq F \subseteq L$ sottocampo $\implies$ $F \subseteq L$ di Galois (perché $K \subseteq L$ di Galois).
- Per dimostrare il punto 2, ricordiamo che $K \subseteq F$ è normale (e quindi di Galois) $\iff$ $F$ è $G$-stabile.
- $K \subseteq F$ normale $\implies$ $f \colon G \to \mathrm{G}_K(F)$, $\sigma \mapsto \sigma|_F$ ben definita. Chiaramente $f$ omomorfismo e $\ker(f) = H$, per cui $H \lhd G$ e $G/H \cong \mathrm{im}(f)$ per il primo teorema di isomorfismo. Inoltre

$$\#\,\mathrm{im}(f) = \#(G/H) = \frac{\#G}{\#H} = \frac{\#[L:K]}{\#[L:F]} = [F:K] = \#\mathrm{G}_K(F),$$

  $\implies$ $f$ suriettiva e $\mathrm{G}_K(F) \cong G/H$.
- $H \lhd G$ $\implies$ $\sigma(\alpha) \in F$ $\forall\, \sigma \in G$ e $\forall\, \alpha \in F$ (quindi $K \subseteq F$ normale): $\sigma(\alpha) \in F = L^H$ $\iff$ $\tau(\sigma(\alpha)) = \sigma(\alpha)$ $\forall\, \tau \in H$ $\iff$ $(\sigma^{-1}\tau\sigma)(\alpha) = \alpha$ $\forall\, \tau \in H$, vero perché $\sigma^{-1}\tau\sigma \in H$ e $\alpha \in F = L^H$.

# Esempio

$K := \mathbb{Q}$ e $L := \mathbb{Q}(\sqrt[3]{2}, \omega)$ con $1 \neq \omega \in \mathbb{C}$ tale che $\omega^3 = 1$.

- $\mathbb{Q} \subset L$ di Galois (è campo di spezzamento di $X^3 - 2$) e $G := \mathrm{G}_{\mathbb{Q}}(L) = \mathrm{G}(L)$ tale che $\#G = [L : \mathbb{Q}] = 6$.
- $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non normale $\implies$ $\mathrm{G}_{\mathbb{Q}(\sqrt[3]{2})}(L) < G$ non normale $\implies$ $G \cong S_3$.
- $\exists!\, H \triangleleft G$ non banale (di ordine 3) $\implies$ $[L : L^H] = 3$, $\mathbb{Q} \subset L^H$ normale e $\mathrm{G}_{\mathbb{Q}}(L^H) \cong G/H \cong C_2$ $\implies$ $L^H = \mathbb{Q}(\omega)$.
- $G$ ha anche 3 sottogruppi non normali non banali (di ordine 2), che corrispondono a $\mathbb{Q}(\omega^i \sqrt[3]{2})$ per $i = 0, 1, 2$.

## Osservazione

- $K \subseteq L$ di Galois $\implies$ $\#\{F : K \subseteq F \subseteq L \text{ sottocampo}\} < \infty$ perché coincide con $\#\{H : H < \mathrm{G}_K(L)\}$.
- $K \subseteq L$ finita $\implies$ $\#\mathrm{G}_K(L) \leq [L : K] < \infty$ $\implies$ $L^{\mathrm{G}_K(L)} \subseteq L$ di Galois e $\#\mathrm{G}_K(L) = [L : L^{\mathrm{G}_K(L)}] \mid [L : K]$ (perché $K \subseteq L^{\mathrm{G}_K(L)} \subseteq L$, quindi $[L : K] = [L : L^{\mathrm{G}_K(L)}][L^{\mathrm{G}_K(L)} : K]$).

# Il gruppo di Galois di un polinomio

## Definizione

$K$ campo, $0 \neq f \in K[X]$. Il gruppo di Galois di $f$ su $K$ (ben definito a meno di isomorfismo) è $\mathrm{G}_K(f) := \mathrm{G}_K(L)$ con $K \subseteq L$ campo di spezzamento di $f$.

## Osservazione

$K \subseteq L$ campo di spezzamento di $f \in K[X] \setminus \{0\}$, $G := \mathrm{G}_K(f)$.

- $K$ perfetto $\implies$ $K \subseteq L$ di Galois $\implies$ $\#G = [L : K]$.
- $R := \{\alpha \in L : f(\alpha) = 0\}$ $\implies$ $n := \#R \leq \deg(f)$.
  $\sigma \in G$, $\alpha \in R$ $\implies$ $\sigma(\alpha) \in R$, quindi si ottiene una funzione $G \to S(R) \cong S_n$, $\sigma \mapsto \sigma|_R$, che è un omomorfismo iniettivo (perché $L = K(R)$) $\implies$ $G \cong G' < S_n$ ($\implies$ $\#G \mid n!$).
- $K$ perfetto, $f$ irriducibile $\implies$ $\deg(f) = n$ e $n \mid \#G \mid n!$.

# Esempi

$K$ perfetto, $f \in K[X]$ irriducibile, $n := \deg(f)$, $G := \mathrm{G}_K(f)$.

- $n = 2 \implies 2 \mid \#G \mid 2! \implies \#G = 2 \implies G \cong C_2$.
- $n = 3 \implies 3 \mid \#G \mid 3! \implies \#G = 3 \text{ o } 6 \implies G \cong C_3 \text{ o } S_3$ (perché $G \cong G' < S_3$).

  $f = X^3 - 2 \implies G \cong S_3$ se $K = \mathbb{Q}$, $G \cong C_3$ se $K = \mathbb{Q}(\omega)$.
- $n = 4 \implies 4 \mid \#G \mid 4! \implies \#G = 4, 8, 12 \text{ o } 24 \implies$ $G \cong C_4$, $C_2^2$, $D_4$, $A_4$ o $S_4$ (perché $G \cong G' < S_4$).

  $f = X^4 - 10X^2 + 1 = \mathrm{m}_{\alpha,\mathbb{Q}}$ con $\alpha = \sqrt{2} + \sqrt{3} \implies G \cong C_2^2$: $\mathbb{Q} \subset \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ normale (perché campo di spezzamento di $(X^2 - 2)(X^2 - 3)$) $\implies$ $f$ si spezza su $\mathbb{Q}(\alpha)$ $\implies$ $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ campo di spezzamento di $f$ $\implies$ $G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \implies \#G = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$ e $G \ncong C_4$ perché $\sigma \in G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \implies$ $\sigma(\sqrt{2}) = \pm\sqrt{2}$ e $\sigma(\sqrt{3}) = \pm\sqrt{3} \implies \sigma^2(\sqrt{2}) = \sqrt{2}$ e $\sigma^2(\sqrt{3}) = \sqrt{3} \implies \sigma^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$.

# Campi finiti

$K$ campo finito $\implies \mathrm{char}(K) = p$ primo.
$0 < n := [K : \mathbb{F}_p] < \infty \implies K \cong \mathbb{F}_p^n$ come $\mathbb{F}_p$-spazio vettoriale (quindi $K \cong C_p^n$ come gruppo abeliano) $\implies \#K = p^n$.

## Teorema

$\forall\, p$ *primo e* $\forall\, n > 0\ \exists!$ *a meno di isomorfismo un campo* $\mathbb{F}_{p^n}$ *di ordine* $p^n$*; inoltre* $\mathbb{F}_{p^n}$ *è campo di spezzamento di* $X^{p^n} - X$ *su* $\mathbb{F}_p$*.*

## Dimostrazione.

$\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ campo di spezzamento di $X^{p^n} - X \implies$
$R := \{\alpha \in \mathbb{F}_{p^n} : \alpha \text{ radice di } X^{p^n} - X\} = \{\alpha \in \mathbb{F}_{p^n} : \mathcal{F}^n(\alpha) = \alpha\}$ sottocampo di $\mathbb{F}_{p^n} \implies \mathbb{F}_{p^n} = \mathbb{F}_p(R) = R$.
$(X^{p^n} - X)' = -1$ non ha radici $\implies X^{p^n} - X$ non ha radici multiple $\implies \#\mathbb{F}_{p^n} = \#R = \deg(X^{p^n} - X) = p^n$.
$K$ altro campo di ordine $p^n \implies \alpha^{p^n - 1} = 1\ \forall\, \alpha \in K^*$ (per il teorema di Lagrange) $\implies$ ogni elemento di $K$ è radice di $X^{p^n} - X$ $\implies \prod_{\alpha \in K}(X - \alpha) \mid (X^{p^n} - X) \implies X^{p^n} - X = \prod_{\alpha \in K}(X - \alpha)$ $\implies \mathbb{F}_p \subseteq K$ campo di spezzamento di $X^{p^n} - X$.

# Gruppi di Galois di estensioni di campi finiti

Se $n, m > 0$, esiste un'estensione $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$:

$\implies$ $d := [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] \implies \mathbb{F}_{p^m} \cong \mathbb{F}_{p^n}^d$ (come $\mathbb{F}_{p^n}$-spazi vettoriali)
$\implies p^m = \#\mathbb{F}_{p^m} = \#\mathbb{F}_{p^n}^d = (p^n)^d = p^{nd} \implies m = nd$;

$\impliedby$ $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \mathcal{F}^n(\alpha) = \alpha\} \subseteq \mathbb{F}_{p^m}$ perché, se $\mathcal{F}^n(\alpha) = \alpha$, allora $\mathcal{F}^m(\alpha) = (\mathcal{F}^n)^{m/n}(\alpha) = \alpha$.

## Corollario

$n \mid m \implies \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ *di Galois e* $\mathrm{G}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^m}) = \langle \mathcal{F}^n \rangle \cong C_{m/n}$.

## Dimostrazione.

$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ è di Galois perché campo di spezzamento di $X^{p^m} - X$ (e $\mathbb{F}_{p^n}$ è perfetto) $\implies \#\mathrm{G}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^m}) = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = m/n$.
$\mathbb{F}_{p^n} = \{\alpha \in \mathbb{F}_{p^m} : \mathcal{F}^n(\alpha) = \alpha\} \implies \mathcal{F}^n \in \mathrm{G}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^m})$, e basta dimostrare $\mathrm{ord}(\mathcal{F}^n) \geq m/n$, cioè $\mathrm{ord}(\mathcal{F}) \geq m$ in $\mathrm{G}(\mathbb{F}_{p^m})$, vero perché $0 < i < m \implies$
$\#\{\alpha \in \mathbb{F}_{p^m} : \mathcal{F}^i(\alpha) = \alpha^{p^i} = \alpha\} \leq p^i < p^m \implies \mathcal{F}^i \neq \mathrm{id}_{\mathbb{F}_{p^m}}$. □

# Gruppi di Galois di polinomi su campi finiti

$p$ primo, $n > 0$, $q := p^n$, $0 \neq f \in \mathbb{F}_q[X]$, $G := \mathrm{G}_{\mathbb{F}_q}(f)$.

- $f$ irriducibile, $d := \deg(f) \implies \mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di $f$ ($\implies G \cong C_d$):
  $\alpha \in \overline{\mathbb{F}}_p$ radice di $f \implies [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d \implies \mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$.
- in generale $f = \prod_{i=1}^{k} f_i$ con $f_i$ irriducibile, $d_i := \deg(f_i)$ $\forall\, i = 1, \ldots, k \implies d := \mathrm{mcm}(d_1, \ldots, d_k)$ tale che $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di $f$ ($\implies G \cong C_d$):
  per il punto precedente $\mathbb{F}_{q^{d_i}}$ è campo di spezzamento di $f_i$ su $\mathbb{F}_q$, quindi $f$ si spezza su $\mathbb{F}_{q^{d'}} \iff \mathbb{F}_{q^{d_i}} \subseteq \mathbb{F}_{q^{d'}}$ $\forall\, i = 1, \ldots, k$ $\iff d_i \mid d'$ $\forall\, i = 1, \ldots, k \iff d \mid d'$.

# Il gruppo di Galois di $X^n - 1$

$n > 0$, $\mathrm{char}(K) \nmid n$, $K \subseteq L$ campo di spezzamento di $X^n - 1$.

- $(X^n - 1)' = nX^{n-1} \neq 0$ ha solo la radice 0 (che non è radice di $X^n - 1$) $\implies$ $X^n - 1$ non ha radici multiple in $L$ $\implies$ $R := \{\alpha \in L : \alpha^n = 1\}$ tale che $\#R = n$.
- $R < L^*$ $\implies$ $R$ ciclico $\implies$ $\exists \omega \in R$ tale che $R = \langle \omega \rangle$ (quindi $\mathrm{ord}(\omega) = n$ in $L^*$, e si dice che $\omega$ è una radice $n$-esima primitiva dell'unità; per esempio $\omega = e^{(2\pi i)/n}$ se $K \subseteq \mathbb{C}$).
- $L = K(R) = K(\omega)$ $\implies$ $\#\mathrm{G}_K(L) = \#R'$ con $R' := \{\alpha \in L : \mathrm{m}_{\omega,K}(\alpha) = 0\} \subseteq R$ (perché $\mathrm{m}_{\omega,K} \mid (X^n - 1)$).
- $\mathrm{m}_{\omega,K}$ si spezza su $L$ e non ha radici multiple $\implies$ $\#\mathrm{G}_K(L) = \deg(\mathrm{m}_{\omega,K}) = [L : K]$ $\implies$ $K \subseteq L$ di Galois.
- La funzione $\mathrm{G}_K(L) \to \mathrm{Aut}(R) < S(R)$, $\sigma \mapsto \sigma|_R$ è ben definita e è un omomorfismo iniettivo di gruppi.
- $\mathrm{G}_K(X^n - 1) = \mathrm{G}_K(L) \cong G < \mathbb{Z}/n\mathbb{Z}^* \cong \mathrm{Aut}(R)$ $\implies$ $G$ abeliano e $\#G \mid \varphi(n)$.

# Polinomi ciclotomici

$\alpha \in R' \implies \exists \sigma \in \mathrm{G}_K(L)$ tale che $\alpha = \sigma(\omega) \implies$
$\mathrm{ord}(\alpha) = \mathrm{ord}(\omega) = n \implies \exists \bar{j} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\alpha = \omega^j \implies$

$$\mathrm{m}_{\omega,K} = \prod_{\alpha \in R'} (X - \alpha) \mid \Phi_n := \prod_{\bar{j} \in \mathbb{Z}/n\mathbb{Z}^*} (X - \omega^j) \in L[X],$$

dove $\Phi_n$ è detto $n$-esimo polinomio ciclotomico. Chiaramente

$$\Phi_n \mid (X^n - 1) = \prod_{\bar{j} \in \mathbb{Z}/n\mathbb{Z}} (X - \omega^j)$$

e $\deg(\Phi_n) = \varphi(n)$.

## Teorema

1. $\Phi_n \in K[X]$.
2. $K = \mathbb{Q} \implies \Phi_n \in \mathbb{Q}[X]$ *irriducibile.*

## Corollario

$\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n$ *e* $\mathrm{G}_{\mathbb{Q}}(X^n - 1) \cong \mathbb{Z}/n\mathbb{Z}^*$.

# Discriminante di un polinomio

- $K$ campo, $0 \neq f \in K[X]$, $K \subseteq L$ campo di spezzamento di $f$.
- $n := \deg(f)$, $\alpha_1, \ldots, \alpha_n \in L$ radici di $f \implies$

$$\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in L$$

è ben definito a meno del segno (dipende dall'ordine delle radici), e chiaramente $\delta \neq 0 \iff f$ non ha radici multiple.

- Il discriminante di $f$ è $\Delta = \Delta(f) := \delta^2 \in L$ (ben definito e tale che $\Delta \neq 0 \iff f$ non ha radici multiple).

## Osservazione

$\sigma(\delta) = \varepsilon(\sigma|_R)\delta$ (con $R := \{\alpha_1, \ldots, \alpha_n\}$) $\forall\, \sigma \in \mathrm{G}_K(f) = \mathrm{G}_K(L)$: posso supporre $\delta \neq 0$ (quindi $\#R = n$), e allora per definizione di segno di una permutazione in $S(R) \cong S_n$

$$\sigma(\delta) = \prod_{1 \leq i < j \leq n} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{1 \leq i < j \leq n} (\sigma|_R(\alpha_i) - \sigma|_R(\alpha_j)) = \varepsilon(\sigma|_R)\delta.$$

# Proprietà del discriminante

## Proposizione

*$K$ perfetto $\implies$ $\Delta = \Delta(f) \in K$. Se inoltre $\mathrm{char}(K) \neq 2$, $f$ non ha radici multiple e identifico $\mathrm{G}_K(f)$ a un sottogruppo di $S_n \cong S(R)$, allora $\mathrm{G}_K(f) \subseteq A_n \iff \delta \in K \iff \Delta$ è un quadrato in $K$.*

## Dimostrazione.

- $K \subseteq L$ di Galois $\implies K = L^{\mathrm{G}_K(L)}$. Dunque, dato $\alpha \in L$, $\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \mathrm{G}_K(L) = \mathrm{G}_K(f)$.
- $\sigma(\Delta) = \sigma(\delta^2) = \sigma(\delta)^2 = (\varepsilon(\sigma|_R)\delta)^2 = \varepsilon(\sigma|_R)^2\delta^2 = \delta^2 = \Delta$ $\forall \sigma \in \mathrm{G}_K(f) \implies \Delta \in K$.
- $\mathrm{G}_K(f) \subseteq A_n \implies \sigma(\delta) = \delta \ \forall \sigma \in \mathrm{G}_K(f) \implies \delta \in K$.
- $\delta \in K$, $f$ senza radici multiple $\implies \delta \in K^*$ e $\forall \sigma \in \mathrm{G}_K(f)$ $\delta = \sigma(\delta) = \varepsilon(\sigma|_R)\delta \implies \varepsilon(\sigma|_R)_K = 1_K \implies \varepsilon(\sigma|_R) = 1$ (cioè $\mathrm{G}_K(f) \subseteq A_n$) se $\mathrm{char}(K) \neq 2$.
- Chiaramente $\delta \in K \iff \Delta = \delta^2$ è un quadrato in $K$.

# Discriminante dei polinomi di grado 2 e 3

- Si può dimostrare che $\Delta(f)$ è esprimibile come polinomio valutato nei coefficienti di $f$.
- $\Delta(X^2 + aX + b) = a^2 - 4b$:

  $X^2 + aX + b = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \implies$
  $a = -\alpha - \beta,\ b = \alpha\beta;$
  $\delta = \alpha - \beta \implies \Delta = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b.$
- $\Delta(X^3 + aX + b) = -4a^3 - 27b^2$:

  $X^3 + aX + b = (X - \alpha)(X - \beta)(X - \gamma) =$
  $X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)X - \alpha\beta\gamma \implies$
  $\alpha + \beta + \gamma = 0,\ a = \alpha\beta + \alpha\gamma + \beta\gamma,\ b = -\alpha\beta\gamma \implies$
  $a = -(\alpha^2 + \alpha\beta + \beta^2),\ b = \alpha\beta(\alpha + \beta);$
  $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = (\alpha - \beta)(2\alpha + \beta)(\alpha + 2\beta) =$
  $2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 \implies$
  $\Delta = (2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3)^2 = 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 -$
  $26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 = -4a^3 - 27b^2.$

# Gruppo di Galois di un polinomio di grado 3

$K$ perfetto, $\mathrm{char}(K) \neq 2$, $\deg(f) = 3$, $f$ irriducibile in $K[X] \implies$

$$\mathrm{G}_K(f) \cong \begin{cases} C_3 & \text{se } \Delta(f) \text{ è un quadrato in } K \\ S_3 & \text{altrimenti.} \end{cases}$$

## Esempio

- $f = X^3 - 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\implies \Delta = -4(-3)^3 - 27 \cdot 1^2 = 81 = 9^2 \implies \mathrm{G}_{\mathbb{Q}}(f) \cong C_3$.
- $f = X^3 + 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\implies \Delta = -4 \cdot 3^3 - 27 \cdot 1^2 = -135 < 0 \implies \mathrm{G}_{\mathbb{Q}}(f) \cong S_3$.

## Osservazione

$\mathrm{char}(K) \neq 3$, $f(X) = X^3 + aX^2 + bX + c \in K[X] \implies$ con la sostituzione $X = Y - a/3$ si ottiene $f(X) = f(Y - a/3) =: g(Y)$ con $g(Y) = Y^3 + a'Y + b' \in K[Y]$. Chiaramente $\alpha \in L$ (campo di spezzamento di $f$ su $K$) è radice di $g \iff \alpha - a/3$ è radice di $f \implies L$ è campo di spezzamento di $g$ su $K \implies \mathrm{G}_K(f) \cong \mathrm{G}_K(g)$.

# Esercizio sui campi finiti

Determinare il gruppo di Galois $G$ di $f := X^5 - X + 3$ su $\mathbb{F}_q$ per $q = 2, 3, 4, 5$.

In ogni caso $G \cong C_d$ se $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di $f$, e $d = \mathrm{mcm}(d_1, \ldots, d_r)$ se $f = \prod_{i=1}^{r} f_i$ con $f_1, \ldots, f_r$ irriducibili.

$q = 2$ $f$ non ha radici (perché $f(\bar{0}) = f(\bar{1}) = \bar{1}$), ma è divisibile per $X^2 + X + 1$ (l'unico irriducibile di grado 2 in $\mathbb{F}_2[X]$) e risulta $f = (X^2 + X + 1)(X^3 + X^2 + 1) \implies d = \mathrm{mcm}(2, 3) = 6$.

$q = 3$ $f = X^5 - X = X(X - 1)(X + 1)(X^2 + 1) \implies d = 2$.

$q = 4$ $\mathbb{F}_{2^6 = 4^3}$ campo di spezzamento di $f$ su $\mathbb{F}_2 \implies$ anche su $\mathbb{F}_4$ $\implies d = 3$.

$q = 5$ $\alpha \in \mathbb{F}_{5^d} \implies f(\alpha) = \mathcal{F}(\alpha) - \alpha + \bar{3} \implies f(a) = \bar{3} \neq \bar{0}$ se $a \in \mathbb{F}_5$ e $f(\alpha + a) = f(\alpha)\ \forall\, \alpha \in \mathbb{F}_{5^d}$ e $\forall\, a \in \mathbb{F}_5 \implies$ $\mathbb{F}_{5^d} = \mathbb{F}_5(\alpha)$ se $\alpha$ radice di $f \implies d = \deg(\mathrm{m}_{\alpha, \mathbb{F}_5})$ non dipende dalla radice $\alpha$ di $f \implies f$ irriducibile in $\mathbb{F}_5[X]$ (non ha radici in $\mathbb{F}_5$ e non può essere $f = gh$ in $\mathbb{F}_5[X]$ con $\deg(g) = 2$ e $\deg(h) = 3$) $\implies d = 5$.

# Esercizio sul gruppo di Galois di $X^n - 2$

$n > 1$, $\alpha := \sqrt[n]{2} \in \mathbb{R}_{>0}$, $\omega := e^{(2\pi i)/n} \in \mathbb{C}$, $G := \mathrm{G}_{\mathbb{Q}}(X^n - 2)$.

1. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \omega)$ campo di spezzamento di $X^n - 2$.
2. $n$ primo $\implies \#G = n\varphi(n) = n(n-1)$.
3. $n = 4$ o $6 \implies \#G = n\varphi(n)$.
4. $n = 8 \implies \#G < n\varphi(n)$.
5. $\#G = n\varphi(n) \implies G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta\colon \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n)$ isomorfismo.

1. Le radici in $\mathbb{C}$ di $X^n - 2$ sono $\alpha\omega^j$ per $j = 0, \ldots, n-1 \implies$ il campo di spezzamento in $\mathbb{C}$ di $X^n - 2$ su $\mathbb{Q}$ è $L := \mathbb{Q}(\alpha\omega^j \,:\, j = 0, \ldots, n-1) = \mathbb{Q}(\alpha, \omega)$.
2. $\mathbb{Q} \subseteq L$ di Galois, $G = \mathrm{G}_{\mathbb{Q}}(L) \implies \#G = [L : \mathbb{Q}]$.
   $X^n - 2$ irriducibile per Eisenstein $\implies \mathrm{m}_{\alpha,\mathbb{Q}} = X^n - 2 \implies$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^n - 2) = n$.
   $\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n \implies [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = n - 1$.
   $\mathrm{mcd}(n, n-1) = 1 \implies [L : \mathbb{Q}] = n(n-1)$.

# Dimostrazione di 3, 4 e 5

3. $\varphi(4) = \varphi(6) = 2 \implies [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = 2 \implies$
   $n = \mathrm{mcm}(n, 2) \mid [L : \mathbb{Q}] \leq 2n \implies [L : \mathbb{Q}] = 2n = n\varphi(n)$
   (altrimenti $[L : \mathbb{Q}] = n \implies \omega \in L = \mathbb{Q}(\alpha) \subset \mathbb{R}$, assurdo).
4. $\omega = \sqrt{2}(1+i)/2$, $\omega^2 = i \implies \sqrt{2}\omega = 1 + i = 1 + \omega^2 \implies \omega$
   radice di $X^2 - \sqrt{2}X + 1 \in \mathbb{Q}(\alpha)[X]$ (perché $\sqrt{2} = \alpha^4$) $\implies$
   $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2 \cdot 8 = 16 < 32 = 8\varphi(8)$.
5. $H := \mathrm{G}_{\mathbb{Q}(\alpha)}(L) < G$ tale che $\#H = \#G/[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(n)$,
   $H' := \mathrm{G}_{\mathbb{Q}(\omega)}(L) \triangleleft G$ (perché $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ normale) tale che
   $\#H' = \#G/[\mathbb{Q}(\omega) : \mathbb{Q}] = n$ e $H \cap H' = \{1\} \implies$
   $\#(HH') = n\varphi(n) = \#G \implies G = HH' \implies G = H' \rtimes H$.
   $H' = \{\sigma_{\bar{j}} : \bar{j} \in \mathbb{Z}/n\mathbb{Z}\}$ con $\sigma_{\bar{j}}(\alpha) = \alpha\omega^j$ (e $\sigma_{\bar{j}}(\omega) = \omega$) $\implies$
   $\sigma_{\bar{j}} = \sigma_{\bar{1}}^j \ \forall \bar{j} \in \mathbb{Z}/n\mathbb{Z} \implies H' = \langle \sigma_{\bar{1}} \rangle \cong C_n$.
   $H \cong G/H' \cong \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}/n\mathbb{Z}^* \implies G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$
   con $\theta \colon \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^*$ omomorfismo iniettivo
   (quindi isomorfismo) perché $\tau \in H \implies \exists\, \bar{l} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che
   $\tau(\omega) = \omega^l$ (e $\tau(\alpha) = \alpha$) $\implies \tau\sigma_{\bar{1}}\tau^{-1} = \sigma_{\bar{l}} = \sigma_{\bar{1}} \iff \tau = 1$

# Esercizio sui polinomi con gruppo di Galois $S_n$

$K$ campo, $0 \neq f \in K[X]$ tale che $\deg(f) = n > 0$ e $\mathrm{G}_K(f) \cong S_n$; $\alpha$ radice di $f$ (in un campo di spezzamento $L$ di $f$ su $K$).

1. $f$ è irriducibile in $K[X]$.
2. $n > 2 \implies \mathrm{G}_K(K(\alpha)) = \{1\}$.
3. $n > 3 \implies \alpha^n \notin K$.

1. $\mathrm{G}_K(f) \cong S_n \implies$ le radici $\alpha = \alpha_1 \ldots, \alpha_n \in L$ di $f$ sono distinte e $\forall\, i = 1, \ldots, n\ \exists\, \sigma \in \mathrm{G}_K(f)$ tale che $\sigma(\alpha) = \alpha_i$ $\implies$ $\alpha_i$ radice di $\mathrm{m}_{\alpha,K} \implies f \mid \mathrm{m}_{\alpha,K} \implies f$ irriducibile.
2. $\sigma \in \mathrm{G}_K(K(\alpha)) \implies \exists\, i = 1, \ldots, n$ tale che $\sigma(\alpha) = \alpha_i$, e basta dimostrare $i = 1$. Per assurdo $i = 2 \implies K(\alpha) \subseteq L$ campo di spezzamento di $\prod_{i=3}^{n}(X - \alpha_i) \implies$ $[L : K] = [L : K(\alpha)][K(\alpha) : K] \leq (n-2)!n < n!$, assurdo perché $[L : K] \geq \#\mathrm{G}_K(L) = n!$.
3. Per assurdo $\alpha^n = a \in K \implies$ posso supporre $f = X^n - a$ $\implies$ $L = K(\alpha, \omega)$ con $\langle \omega \rangle = \{\beta \in L : \beta^n = 1\} < L^* \implies$ $[L : K] \leq [K(\alpha) : K][K(\omega) : K] \leq n(n-1) < n!$, assurdo.

# Esercizio sui gruppi di Galois di polinomi biquadratici

Determinare campo di spezzamento $\mathbb{Q} \subseteq L$ e gruppo di Galois $G$ di $f$ su $\mathbb{Q}$ nei seguenti casi:

1. $f = X^4 - 4X^2 + 2$;
2. $f = X^4 - 4X^2 - 2$.

1. $f$ irriducibile per Eisenstein.
   $f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y + 2$ che ha radici $2 \pm \sqrt{2} \in \mathbb{R}_{>0} \implies$ le radici di $f$ sono $\pm\alpha, \pm\beta$ con $\alpha := \sqrt{2+\sqrt{2}}, \beta := \sqrt{2-\sqrt{2}} \in \mathbb{R}_{>0} \implies L = \mathbb{Q}(\alpha, \beta)$.
   $\alpha^2 - 2 = \sqrt{2} = \alpha\beta \implies \beta = (\alpha^2 - 2)/\alpha \in \mathbb{Q}(\alpha) \implies$
   $L = \mathbb{Q}(\alpha) \implies \#G = [L : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$.
   $\exists \sigma \in G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ tale che $\sigma(\alpha) = \beta$ (perché $\beta$ radice di $\mathrm{m}_{\alpha,\mathbb{Q}} = f$) $\implies$

$$\sigma^2(\alpha) = \sigma(\beta) = \sigma\left(\frac{\alpha^2 - 2}{\alpha}\right) = \frac{\beta^2 - 2}{\beta} = \frac{-\sqrt{2}}{\beta} = -\alpha$$

$\implies \sigma^2 \neq \mathrm{id}_L \implies G \cong C_4$.

# Dimostrazione di 2

$f$ irriducibile per Eisenstein.
$f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y - 2$ che ha radici
$2 \pm \sqrt{6} \in \mathbb{R} \implies$ le radici di $f$ sono $\pm\alpha, \pm\beta i$ con
$\alpha := \sqrt{\sqrt{6}+2}, \beta := \sqrt{\sqrt{6}-2} \in \mathbb{R}_{>0} \implies L = \mathbb{Q}(\alpha, \beta i)$.
$\alpha\beta = \sqrt{2} \implies \alpha\beta i = \sqrt{2} i \implies L = \mathbb{Q}(\alpha, \sqrt{2} i)$.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$,
$[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = \deg(\mathrm{m}_{\sqrt{2}i,\mathbb{Q}}) = 2$ (perché $\mathrm{m}_{\sqrt{2}i,\mathbb{Q}} = X^2 + 2$) $\implies$

$$\mathrm{mcm}(4, 2) = 4 \mid \#G = [\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] \leq 4 \cdot 2 = 8$$

e non può essere $[\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] = 4$ (perché $\sqrt{2}i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$)
$\implies \#G = 8$.
$G \cong G' < S_4 \implies G \cong D_4$.