Complementi di Algebra

Alessio Borzì

Indice

Teoria dei campi

1.1 Alcuni richiami di algebra

Lemma 1.1.1. *Sia $\phi : A \to B$ un omomorfismo di anelli con A anello unitario e B dominio unitario. Se ϕ non è l'omomorfismo nullo allora $\phi(1_A) = 1_B$.*

Dimostrazione.

$$\phi(1_A) = \phi(1_A \cdot 1_A) = \phi(1_A) \cdot \phi(1_A)$$

da cui essendo $\phi(1_A) \neq 0$ (ϕ diverso è dall'omomorfismo nullo) e dalla legge dell'annullamento del prodotto (valida in B in quanto dominio) otteniamo $\phi(1_A) = 1_B$. □

Corollario 1.1.2. *Se $\mathbb{F}$ è un sottocampo di $\mathbb{K}$ allora $1_{\mathbb{F}} = 1_{\mathbb{K}}$*

Dimostrazione. Basta utilizzare il lemma precedente considerando l'inclusione canonica $i : \mathbb{F} \to \mathbb{K}$ con $i(\alpha) = \alpha \quad \forall \alpha \in \mathbb{F} \subseteq \mathbb{K}$. □

Definizione 1.1.3. *Sia A un anello unitario, definiamo la funzione $\phi : \mathbb{Z} \to A$ con*

$$\phi(n) = \begin{cases} n \cdot 1_A & n > 0 \\ 0 & n = 0 \\ -\phi(-n) & n < 0 \end{cases}$$

(dove, se $n \in \mathbb{Z}$ e $a \in A$, intendiamo $n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ volte}}$).
*É facile verificare che ϕ è un omomorfismo di anelli e risulta immediatamente che $\phi(1) = 1_A$. Quindi il nucleo di ϕ è un ideale di $\mathbb{Z}$, in simboli $\ker\phi \trianglelefteq \mathbb{Z}$, ma ricordando che $\mathbb{Z}$ è un anello a ideali principali (PID) deve esistere un intero $r \geq 0$ tale che $\ker\phi = (r)$. L'intero r è detto **caratteristica** dell'anello A, e verrà indicata con $ch(A) = r$.*

Osservazione 1.1.4. *La caratteristica di A è il più piccolo intero $r \geq 0$ tale che $r \cdot a = 0 \quad \forall a \in A$, in quanto r genera $\ker\phi$ e inoltre, dato che $r \cdot 1_A = 0$, si ha*

$$r \cdot a = r \cdot (1_A \cdot a) = (r \cdot 1_A) \cdot a = 0 \cdot a = 0.$$

Osserviamo inoltre che vale anche il viceversa, cioè che il più piccolo intero $r \geq 0$ tale che $r \cdot a = 0 \quad \forall a \in A$ coincide con $ch(A)$.

Proposizione 1.1.5. *Se A è un dominio allora $ch(A)$ è uguale a 0 oppure a un intero p primo.*

Dimostrazione. Considerando $\phi : \mathbb{Z} \to A$ abbiamo che $\operatorname{Im}\phi \leq A$, quindi $\operatorname{Im}\phi$ risulterà anch'essa un dominio. In base al primo teorema dell'isomorfismo abbiamo

$$\mathbb{Z}/\ker\phi \simeq \operatorname{Im}\phi$$

dunque $\ker\phi$ è un ideale primo di $\mathbb{Z}$ in quanto $\operatorname{Im}\phi$ è un dominio. Allora $\ker\phi$ risulterà uguale all'ideale nullo (0), in questo caso $ch(A) = 0$, oppure $\ker\phi = (p)$ con $p \geq 0$ intero primo, in questo caso $ch(A) = p$. □

Lemma 1.1.6. *Sia A un dominio con $ch(A) = p$ primo, allora*

$$\forall a, b \in A \quad (a+b)^p = a^p + b^p$$

Dimostrazione. Dalla formula del binomio di Newton

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

osserviamo che per ogni $i \in \{1, 2, \ldots, p-1\}$ abbiamo

$$p \nmid i!,\ p \nmid (p-i)!,\ p \mid p! \Rightarrow p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$$

da cui

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

□

Corollario 1.1.7. *Se $\mathbb{K}$ è un campo allora $ch(\mathbb{K})$ è uguale a 0 o p, con p primo.*

Lemma 1.1.8. *Se S e T sono due sottocampi di $\mathbb{K}$ allora $S \cap T \subseteq \mathbb{K}$ è un sottocampo di $\mathbb{K}$.*

Dimostrazione.

- $S \cap T$ è un sottoanello di $\mathbb{K}$;
- in $S \cap T$ vale la proprietà commutativa in quanto vale in $\mathbb{K}$;
- l'unità di S e l'unità di T coincidono con l'unità di $\mathbb{K}$, quindi esse sono uguali tra loro, pertanto l'unità di $\mathbb{K}$ coinciderà a sua volta con l'unità di $S \cap T$;
- per ogni $\alpha \in S \cap T$ esiste l'inverso in S e in T che però è unico in quanto è l'inverso di α anche in $\mathbb{K}$, quindi l'inverso di α apparterrà a $S \cap T$.

□

Definizione 1.1.9. *Si chiama **sotto campo primo** (o **fondamentale**) P di un campo $\mathbb{K}$ il più piccolo sottocampo contenuto in $\mathbb{K}$, o equivalentemente l'intersezione di tutti i sottocampi di $\mathbb{K}$.*

Proposizione 1.1.10. *Sia $\mathbb{K}$ un campo.*

1. *Se $ch(\mathbb{K}) = p$ allora $P \simeq \mathbb{Z}_p$ (con p primo).*
2. *Se $ch(\mathbb{K}) = 0$ allora $P \simeq \mathbb{Q}$.*

Dimostrazione.

1. Se $ch(\mathbb{K}) = p$ allora, considerando $\phi : \mathbb{Z} \to \mathbb{K}$ come definita precedentemente, si ha $\ker \phi = (p)$ quindi
$$\operatorname{Im} \phi \simeq \mathbb{Z}/\ker \phi = \mathbb{Z}/(p) \simeq \mathbb{Z}_p$$
pertanto $\mathbb{Z}_p \simeq \operatorname{Im} \phi \leq \mathbb{K}$, cioè con abuso di notazione $\mathbb{Z}_p \subseteq \mathbb{K}$. Abbiamo così dimostrato che ogni campo di caratteristica p contiene un sottocampo isomorfo a $\mathbb{Z}_p$. Adesso dato che ogni sottocampo di $\mathbb{K}$ avrà anch'esso caratteristica pari a p, dall'affermazione precedente segue che ogni sottocampo di $\mathbb{K}$ contiene una copia isomorfa a $\mathbb{Z}_p$, quindi risulta $P = \mathbb{Z}_p$.

2. Se $ch(\mathbb{K}) = 0$ allora $\ker \phi = (0)$ quindi
$$\operatorname{Im} \phi \simeq \mathbb{Z}/\ker \phi = \mathbb{Z}/(0) \simeq \mathbb{Z}$$
pertanto $\mathbb{Z} \simeq \operatorname{Im} \phi \leq \mathbb{K}$, cioè con abuso di notazione $\mathbb{Z} \subseteq \mathbb{K}$. Adesso consideriamo l'applicazione $\bar{\phi} : \mathbb{Q} \to \mathbb{K}$ con $\bar{\phi}\left(\frac{n}{m}\right) = \phi(n) \cdot \phi(m)^{-1}$. Mostriamo che $\bar{\phi}$ è un'immersione di $\mathbb{Q}$ in $\mathbb{K}$:

   - $\bar{\phi}$ è ben definita. Infatti $\phi(m)$ ha inverso $\forall m \in \mathbb{Z} \setminus \{0\}$. Inoltre se
   $$\frac{n}{m} = \frac{a}{b} \Rightarrow nb = ma \Rightarrow \phi(n)\phi(b) = \phi(m)\phi(a) \Rightarrow$$
   $$\Rightarrow \phi(n)\phi(m)^{-1} = \phi(a)\phi(b)^{-1} \Rightarrow \bar{\phi}\left(\frac{n}{m}\right) = \bar{\phi}\left(\frac{a}{b}\right).$$
   - $\bar{\phi}$ è omomorfismo in quanto lo è ϕ.
   - $\bar{\phi}$ è iniettivo, cioè $\ker \bar{\phi} = \{0_{\mathbb{K}}\}$ infatti sia $\frac{n}{m} \in \ker \bar{\phi}$ allora
   $$\bar{\phi}\left(\frac{n}{m}\right) = \phi(n)\phi(m)^{-1} = 0_{\mathbb{K}} \Rightarrow \phi(n) = 0_{\mathbb{K}} \Rightarrow n = 0 \Rightarrow \frac{n}{m} = 0.$$

   Abbiamo così dimostrato che ogni campo di caratteristica 0 contiene un sottocampo isomorfo a $\mathbb{Q}$. Adesso dato che ogni sottocampo di $\mathbb{K}$ avrà anch'esso caratteristica pari a 0, dall'affermazione precedente segue che ogni sottocampo di $\mathbb{K}$ contiene una copia isomorfa a $\mathbb{Q}$, quindi risulta $P = \mathbb{Q}$.

□

Riportiamo qui un importante teorema senza darne dimostrazione.

Teorema 1.1.11. (Teorema di Ruffini) *Sia $\mathbb{K}$ un campo e $f(x) \in \mathbb{K}[x]$ un polinomio. Se $\alpha \in \mathbb{K}$ è una radice di $f(x)$ (cioè tale che $f(\alpha) = 0$) allora il polinomio $x - \alpha$ divide $f(x)$ in $\mathbb{K}[x]$.*

Definizione 1.1.12. *Sia* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$. *Si chiama* ***derivata formale*** *di* f *il polinomio*[1] $f'(x) = n \cdot a_n x^{n-1} + \cdots + a_2 x + a_1$.

Osserviamo che, se $f, g \in \mathbb{K}[x]$, valgolo le proprietà

1. $(f+g)' = f' + g'$
2. $(f \cdot g)' = f' \cdot g + f \cdot g'$

Definizione 1.1.13. *Sia* $f(x) \in \mathbb{K}[x]$ *un polinomio e* $\alpha \in \mathbb{K}$ *una sua radice, chiamiamo* ***molteplicità*** *di* α *come radice di* f *il massimo intero* m *tale che* $(x-\alpha)^m$ *divida* $f(x)$, *cioè*

$$m = \max\{n \in \mathbb{Z} : (x-\alpha)^n | f(x)\}.$$

Se la radice α *di* f *ha molteplicità* $m > 1$ *allora è detta* ***radice multipla****.*

Proposizione 1.1.14. *Il polinomio* $f(x) \in \mathbb{K}[x]$ *ha* $\alpha \in \mathbb{K}$ *come radice multipla se e solo se* $f(\alpha) = f'(\alpha) = 0$.

Dimostrazione.

$\Rightarrow$ Per ipotesi abbiamo che $f(x) = (x-\alpha)^m \cdot g(x)$ con $m > 1$, quindi

$$f'(x) = m(x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x)$$

da cui $f'(\alpha) = 0$.

$\Leftarrow$ Per ipotesi sappiamo che $f(x) = (x-\alpha) \cdot g(x)$, quindi

$$f'(x) = g(x) + (x-\alpha) \cdot g'(x)$$

sapendo che $f'(\alpha) = 0$ otteniamo $f'(\alpha) = g(\alpha) = 0$, da cui $g(x) = (x-\alpha) \cdot h(x)$, dunque $f(x) = (x-\alpha) \cdot g(x) = (x-\alpha)^2 \cdot h(x)$.

□

1.2 Estensione di Campi

Definizione 1.2.1. *Siano* $\mathbb{F}$ *e* $\mathbb{K}$ *due campi. Se* $\mathbb{F}$ *è un sottocampo di* $\mathbb{K}$ *diremo che* $\mathbb{K}$ *è un'****estensione*** *di* $\mathbb{F}$ *e l'inclusione* $\mathbb{F} \subseteq \mathbb{K}$ *verrà chiamata* ***estensione di campi****.*

Osservazione 1.2.2. *Data l'estensione di campi* $\mathbb{F} \subseteq \mathbb{K}$, $\mathbb{K}$ *può essere visto come* $\mathbb{F}$*-spazio vettoriale una volta definita l'operazione di prodotto esterno*

$$\bullet : \mathbb{F} \times \mathbb{K} \to \mathbb{K} \quad \textit{dove} \quad a \bullet \alpha = a \cdot \alpha \quad \forall a \in \mathbb{F}, \forall \alpha \in \mathbb{K}.$$

Infatti $(\mathbb{K}, +)$ *è ancora un gruppo abeliano, inoltre* $\forall a, b \in \mathbb{F}, \alpha, \beta \in \mathbb{K}$

1. $(a+b) \bullet \alpha = (a+b) \cdot \alpha = a \cdot \alpha + b \cdot \beta = a \bullet \alpha + b \bullet \beta$

[1] Nello scrivere $i \cdot a_i$ con $i \in \mathbb{Z}$ e $a_i \in \mathbb{K}$ stiamo utilizzando ancora una volta la notazione utilizzata in precedenza.

2. $a \bullet (\alpha + \beta) = a \cdot (\alpha + \beta) = a \cdot \alpha + a \cdot \beta = a \bullet \alpha + a \bullet \beta$

3. $(a \cdot b) \bullet \alpha = (a \cdot b) \cdot \alpha = a \cdot (b \cdot \alpha) = a \bullet (b \bullet \alpha)$

4. $1_{\mathbb{F}} \bullet \alpha = 1_{\mathbb{F}} \cdot \alpha = 1_{\mathbb{K}} \cdot \alpha = \alpha$

ciò prova che $\mathbb{K}$ con il prodotto esterno definito in precedenza è un $\mathbb{F}$-spazio vettoriale.

Definizione 1.2.3. *Data l'estensione $\mathbb{F} \subseteq \mathbb{K}$, se $\dim_{\mathbb{F}} \mathbb{K} < \infty$ allora $\mathbb{F} \subseteq \mathbb{K}$ è detta* ***estensione finita****, altrimenti* ***estensione infinita****, inoltre chiamiamo $\dim_{\mathbb{F}} \mathbb{K} = [\mathbb{K} : \mathbb{F}]$* ***grado dell'estensione****.*

Teorema 1.2.4. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e V uno spazio vettoriale su $\mathbb{K}$. Chiaramente V è anche uno spazio vettoriale su $\mathbb{F}$ se consideriamo la restrizione a $\mathbb{F}$ del prodotto esterno. Sotto queste ipotesi abbiamo che $\dim_{\mathbb{F}} V$ è finita se e solo se $\dim_{\mathbb{K}} V$ e $[\mathbb{K} : \mathbb{F}]$ sono finite, in tal caso*

$$\dim_{\mathbb{F}} V = \dim_{\mathbb{K}} V \cdot [\mathbb{K} : \mathbb{F}]$$

Dimostrazione.

$\Rightarrow$ Supponiamo che $\dim_{\mathbb{F}} V = n$, sia $\{v_1, v_2, \ldots, v_n\}$ una base di V su $\mathbb{F}$. Dato che $\mathbb{F} \subseteq \mathbb{K}$ si ha che i vettori v_i generano linearmente V su $\mathbb{K}$ da cui $\dim_{\mathbb{K}} V \leq \dim_{\mathbb{F}} V = n$. Sia adesso $v \in V$, consideriamo il sottospazio $\mathbb{K}v = \{e \cdot v : e \in \mathbb{K}\} \subseteq V$, risulta $[\mathbb{K} : \mathbb{F}] = \dim_{\mathbb{F}} \mathbb{K}v \leq \dim_{\mathbb{F}} V = n$.

$\Leftarrow$ Viceversa, sia $\{v_1, v_2, \ldots, v_h\}$ una base di V su $\mathbb{K}$ e $\{e_1, e_2, \ldots, e_k\}$ una base di $\mathbb{K}$ su $\mathbb{F}$, proviamo che l'insieme di vettori

$$\{e_1v_1, \ldots, e_kv_1, e_1v_2, \ldots, e_kv_2, \ldots, e_1v_h, \ldots, e_kv_h\} = \bigcup_{i=1}^{h} \{e_1v_i, \ldots, e_kv_i\}$$

è una base di V su $\mathbb{F}$. Per fare ciò osserviamo che per un qualunque $v \in V$ possiamo scrivere

$$v = \sum_{i=1}^{h} a_i v_i \quad a_i \in \mathbb{K}$$

inoltre per ogni $a_i \in \mathbb{K}$ possiamo scrivere

$$a_i = \sum_{j=1}^{k} b_{ij} e_j \quad b_{ij} \in \mathbb{F}$$

ottenendo infine

$$v = \sum_{i=1}^{h} a_i v_i = \sum_{i=1}^{h} \sum_{j=1}^{k} b_{ij} e_j v_i$$

da cui segue che i vettori $e_j v_i$ sono un sistema di generatori di V su $\mathbb{F}$, rimane da dimostrare che essi sono linearmente indipendenti. Supponiamo che

$$\sum_{i=1}^{h} \sum_{j=1}^{k} a_{ij} e_j v_i = \underline{0} \quad a_{ij} \in \mathbb{F}$$

ponendo $b_i = \sum_{j=1}^{k} a_{ij}e_j$ otteniamo

$$\sum_{i=1}^{h} b_i v_i = 0$$

da cui dalla lineare indipendenza dei vettori v_i segue che $b_i = 0$ per ogni i, cioè

$$b_i = \sum_{j=1}^{k} a_{ij}e_j = 0$$

in modo analogo, dalla lineare indipendenza dei vettori e_j segue $a_{ij} = 0$ per ogni i e j. Questo prova che i vettori $e_j v_i$ sono una base di V su $\mathbb{F}$, la relazione tra le dimensioni risulta adesso ovvia in quanto la base di V su $\mathbb{F}$ è formata da hk vettori.

□

Un caso particolare del teorema precedente è quando lo spazio vettoriale V considerato è anch'esso un campo.

Corollario 1.2.5. *Se $\mathbb{F}, \mathbb{K}$ e $\mathbb{E}$ sono tre campi tali che $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ allora l'estensione $\mathbb{F} \subseteq \mathbb{E}$ è finita se e solo se lo sono $\mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{E}$, inoltre*

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$$

Definizione 1.2.6. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e siano $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$. Sia $\mathcal{F}$ la famiglia di tutti i sottocampi di $\mathbb{K}$ contenenti $\mathbb{F}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$. Osserviamo che $\mathbb{K} \in \mathcal{F} \neq \emptyset$. Definiamo*

$$\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \bigcap_{T \in \mathcal{F}} T$$

cioè $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ è il più piccolo sottocampo di $\mathbb{K}$ contenente $\mathbb{F}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Proposizione 1.2.7. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{K}$, $B = \{\beta_1, \beta_2, \ldots, \beta_m\} \subseteq \mathbb{K}$, abbiamo*

$$\mathbb{F}(A \cup B) = \mathbb{F}(A)(B)$$

Dimostrazione.

- $\subseteq$ Abbiamo $A \cup B \subseteq \mathbb{F}(A) \cup B \subseteq \mathbb{F}(A)(B) \Rightarrow \mathbb{F}(A \cup B) \subseteq \mathbb{F}(A)(B)$ in quanto $\mathbb{F}(A \cup B)$ è il più piccolo sottocampo di $\mathbb{K}$ che contiene $A \cup B$ ed $\mathbb{F}$.
- $\supseteq$ Analogamente $\mathbb{F}(A) \cup B \subseteq \mathbb{F}(A \cup B) \Rightarrow \mathbb{F}(A)(B) \subseteq \mathbb{F}(A \cup B)$

□

Proposizione 1.2.8. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$. Il campo $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è del tipo*

$$\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} : f, g \in \mathbb{F}[x_1, \ldots, x_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\},$$

cioè $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è il campo delle frazioni di $\mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

Dimostrazione. Chiamiamo l'insieme della tesi Δ.

$\subseteq$ Poiché $\mathbb{F} \subseteq \Delta$ e $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Delta$ basta provare che Δ è un campo.

- Δ è un sottoanello di $\mathbb{K}$ in quanto se $a, b \in \Delta$ allora si verifica facilmente che anche $a - b, a \cdot b \in \Delta$.
- Δ è commutativo in quanto lo è $\mathbb{K}$.
- Δ è unitario poiché $\forall g \in \mathbb{F}[x_1, \ldots, x_n]$ con $g(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ si ha

$$\frac{g(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} = 1_{\mathbb{K}} \in \Delta.$$

- Se $(f/g)(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \Delta \setminus \{0_\Delta\}$ allora $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ quindi $(g/f)(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \Delta$, cioè ogni elemento non nullo ha il suo inverso in Δ.

$\supseteq$ Dato che $\alpha_1, \ldots, \alpha_n \in \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ allora $\forall m_1, m_2, \ldots, m_n \in \mathbb{N}$ abbiamo $\alpha_1^{m_1}, \alpha_2^{m_2}, \ldots, \alpha_n^{m_n} \in \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, quindi $\forall f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ si ha $f(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, inoltre se $f(\alpha_1, \ldots, \alpha_n) \neq 0$ allora anche $f(\alpha_1, \ldots, \alpha_n)^{-1} \in \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, e questo prova che $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) \supseteq \Delta$.

□

Definizione 1.2.9. *Un'estensione $\mathbb{F} \subseteq \mathbb{K}$ è detta **finitamente generata** (f.g.) se $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K} : \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}$. Nel caso in cui $n = 1$ l'estensione è detta **semplice**.*

Proposizione 1.2.10. *Se l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è finita allora è anche finitamente generata.*

Dimostrazione. Per ipotesi $[\mathbb{K} : \mathbb{F}] = n$. Sia $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ una base di $\mathbb{K}$ in $\mathbb{F}$, allora $\forall y \in \mathbb{K}, \exists! y_1, \ldots, y_n \in \mathbb{F} : y = y_1 b_1 + \cdots + y_n b_n$, quindi $y \in \mathbb{F}(b_1, \ldots, b_n)$ cioè $\mathbb{K} \subseteq \mathbb{F}(b_1, \ldots, b_n) \Rightarrow \mathbb{K} = \mathbb{F}(b_1, \ldots, b_n)$. □

Definizione 1.2.11. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Un elemento $\alpha \in \mathbb{K}$ è **algebrico** su $\mathbb{F}$ se $\exists f \in \mathbb{F}[x] \setminus \{\underline{0}\} : f(\alpha) = 0$. Se $\alpha \in \mathbb{K}$ non è algebrico su $\mathbb{F}$ allora è **trascendente** su $\mathbb{F}$.*
Quando diremo che $\alpha \in \mathbb{C}$ è algebrico o trascendente, senza specificare il campo $\mathbb{F}$, intenderemo su $\mathbb{Q}$.

Osservazione 1.2.12. *Ogni $\alpha \in \mathbb{F}$ è algebrico su $\mathbb{F}$ in quanto banalmente α è radice del polinomio $x - \alpha \in \mathbb{F}[x]$. In questo caso $\mathbb{F} = \mathbb{F}(\alpha)$.*

Abbiamo visto che un'estensione finita è finitamente generata. Il seguente esempio mostra che non vale il viceversa.

Esempio 1.2.13. *Consideriamo $\mathbb{Q}$, $\pi \in \mathbb{R}$. L'estensione semplice $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ non è finita. Infatti se per assurdo $[\mathbb{Q}(\pi) : \mathbb{Q}] = n$ allora considero $n + 1$ elementi del tipo $1, \pi, \pi^2, \ldots, \pi^n \in \mathbb{Q}(\pi)$. Essi devono essere linearmente dipendenti, quindi $\exists a_0, a_1, \ldots, a_n \in \mathbb{Q}$ non tutti nulli tali che $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$, contro la trascendenza di π in $\mathbb{Q}$ (che non dimostriamo).*

Definizione 1.2.14. *L'estensione $\mathbb{F} \subseteq \mathbb{K}$ è detta* ***algebrica*** *se ogni $\alpha \in \mathbb{K}$ è algebrico su $\mathbb{F}$.*

Esempio 1.2.15. *L'estensione $\mathbb{R} \subseteq \mathbb{C}$ è algebrica. Infatti ogni numero complesso $\alpha = a + ib \in \mathbb{C}$ $(a, b \in \mathbb{R})$ è algebrico su $\mathbb{R}$ in quanto considerando il polinomio a coefficienti reali*

$$p(x) = x^2 - 2ax + a^2 + b^2 = (x - (a + ib))(x - (a - ib))$$

esso è un polinomio non nullo (il coefficiente di secondo grado è diverso da zero) che si annulla in α.

Teorema 1.2.16. *Ogni estensione $\mathbb{F} \subseteq \mathbb{K}$ finita è anche algebrica.*

Dimostrazione. Per ipotesi $[\mathbb{K} : \mathbb{F}] = n$, allora $\forall \alpha \in \mathbb{K}$ gli elementi $1, \alpha, \ldots, \alpha^n$ sono l.d. su $\mathbb{F}$, quindi $\exists a_0, a_1, \ldots, a_n \in \mathbb{F}$ non tutti nulli tali che $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, cioè posto $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{F}[x] \setminus \{\underline{0}\}$ si ha $f(\alpha) = 0$, quindi α è algebrico su $\mathbb{F}$. Dall'arbitrarietà di α segue che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è algebrica. □

Proposizione-Definizione 1.2.17. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha \in \mathbb{K}$. L'applicazione $\phi_\alpha : \mathbb{F}[x] \to \mathbb{K}$ con $\phi_\alpha(f(x)) = f(\alpha)$ è un omomorfismo di anelli, con*

$$\operatorname{Im} \phi_\alpha = \{f(\alpha) : f(x) \in \mathbb{F}[x]\} = \mathbb{F}[\alpha].$$

Tale omomorfismo è detto ***omomorfismo di valutazione****.*

Dimostrazione. $\forall f, g \in \mathbb{F}[x]$

- $\phi_\alpha(f + g) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)$
- $\phi_\alpha(f \cdot g) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \phi_\alpha(f) \cdot \phi_\alpha(g)$

□

Proposizione-Definizione 1.2.18. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha \in \mathbb{K}$ algebrico su $\mathbb{F}$. Esiste un unico polinomio monico di grado minimo che abbia α come radice e che sia irriducibile in $\mathbb{F}$. Quest'ultimo è detto* ***polinomio minimo*** *di α in $\mathbb{F}$ e si indica con $p_\alpha^{\mathbb{F}}(x)$.*

Dimostrazione. Consideriamo $\ker \phi_\alpha \trianglelefteq \mathbb{F}[x]$. $\mathbb{F}[x]$ è un dominio euclideo con valutazione pari al grado del polinomio. Nei domini euclidei sappiamo che gli ideali sono tutti principali e sono generati dall'elemnto di valutazione minima, quindi $\ker \phi_\alpha = (f(x))$ con $f(x) \neq \underline{0}$ (altrimenti α non sarebbe algebrico su $\mathbb{F}$) di grado minimo su $\ker \phi_\alpha$. Inoltre abbiamo

$$\mathbb{F}[x]/\ker \phi_\alpha \simeq \operatorname{Im} \phi_\alpha \leq \mathbb{K}$$

così facendo $\operatorname{Im} \phi_\alpha$ risulterà un dominio (poiché sottoanello di $\mathbb{K}$), quindi $\ker \phi_\alpha$ sarà un ideale primo di $\mathbb{F}[x]$ e pertanto ogni suo generatore risulterà primo quindi sarà anche irriducibile. Poiché $(f(x)) = (af(x))$ per ogni $a \in \mathbb{F}$ e che l'insieme $\{af(x) : a \in \mathbb{F}\}$ ha un solo polinomio monico (che si ottiene quando a è l'inverso del coefficiente di grado massimo di $f(x)$) segue che esisterà un unico polinomio monico di grado minimo irriducibile di $\ker \phi_\alpha$ (cioè che abbia α come radice). □

Il polinomio minimo di un elemento dipende rispetto a quale campo viene considerato, come mostra il seguente

Esempio 1.2.19. *Consideriamo la seguente estensione $\mathbb{Q} \subseteq \mathbb{C}$. Il polinomio minimo di $i\sqrt[4]{2} \in \mathbb{C}$ in $\mathbb{Q}$ è $x^4 - 2 \in \mathbb{Q}[x]$, mentre il polinomio minimo dello stesso elemento in $\mathbb{Q}(\sqrt{2})$ è $x^2 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.*

Osservazione 1.2.20. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha \in \mathbb{K}$. Se $f \in \mathbb{F}[x]$ è irriducibile, monico ed è tale che $f(\alpha) = 0$ allora $f(x)$ è di grado minimo tale che $f(\alpha) = 0$, cioè è il polinomio minimo di α in $\mathbb{F}$.*

Osservazione 1.2.21. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha, \beta \in \mathbb{K}$. Se α e β hanno lo stesso polinomio minimo $f(x)$ in $\mathbb{F}$ allora*

$$\mathbb{F}[\alpha] = \operatorname{Im} \phi_\alpha \simeq \mathbb{F}[x]/(f(x)) \simeq \operatorname{Im} \phi_\beta = \mathbb{F}[\beta]$$

Proposizione 1.2.22. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\alpha \in \mathbb{K}$ algebrico su $\mathbb{F}$. Gli elementi di $\mathbb{F}[\alpha]$ si esprimono in modo unico nella forma $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ con $a_i \in \mathbb{F}$ e $n = deg(f)$ dove $f \in \mathbb{F}[x]$ è il polinomio minimo di α in $\mathbb{F}$.*

Dimostrazione. Sia $a \in \mathbb{F}[\alpha]$, allora $a = p(\alpha)$ per qualche $p(x) \in \mathbb{F}[x]$. Eseguiamo la divisione euclidea del polinomio p per f:

$$\exists q, r \in \mathbb{F}[x] : \quad p(x) = q(x) \cdot f(x) + r(x)$$

con $r(x) = \underline{0}$ oppure $\deg(r) < \deg(f) = n$, quindi $a = 0$ oppure $a = p(\alpha) = r(\alpha)$ con $\deg(r) < n$. Questo prova l'esistenza degli $a_i \in \mathbb{F}$.
Per l'unicità supponiamo che esistano $a_i, b_i \in \mathbb{F}$ tali che

$$a = \sum_{i=0}^{n-1} a_i\alpha^i = \sum_{i=0}^{n-1} b_i\alpha^i$$

allora consideriamo il polinomio

$$u(x) = \sum_{i=0}^{n-1} (a_i - b_i)x^i$$

per quanto scritto prima abbiamo $u(\alpha) = 0$, inoltre, se u fosse non nullo, si avrebbe $\deg(u) \leq n - 1 < n = \deg(f)$ e questo contraddirebbe la minimalità del grado di f, quindi dev'essere $u = \underline{0}$, cioè $a_i = b_i \quad \forall i \in \{0, \ldots, n-1\}$. □

Teorema 1.2.23. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Un elemento $\alpha \in \mathbb{K}$ è algebrico se e solo se $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.*

Dimostrazione.

- $\Rightarrow$ É ovvio che $\mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha)$. Viceversa, essendo $\mathbb{F}[x]$ un dominio euclideo ogni suo ideale generato da un elemento irriducibile è massiamle, quindi se consideriamo il polinomio minimo $f(x) \in \mathbb{F}[x]$ di α in $\mathbb{F}$ abbiamo che l'ideale $(f(x))$ è massiamle, quindi dato che $\mathbb{F}[\alpha] = \mathbb{F}[x]/(f(x))$, $\mathbb{F}[\alpha]$ è campo. Infine $\mathbb{F}[\alpha]$ contiene sia $\mathbb{F}$ che α quindi $\mathbb{F}(\alpha) \subseteq \mathbb{F}[\alpha]$, da cui l'uguaglianza.

$\Leftarrow$ Per ipotesi si ha $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$, quindi possiamo scrivere

$$\frac{1}{\alpha} \in \mathbb{F}(\alpha) = \mathbb{F}[\alpha] \Rightarrow \frac{1}{\alpha} = \sum_{i=0}^{n-1} a_i \alpha^i \quad a_i \in \mathbb{F}$$

da cui moltiplicando ambo i membri dell'ultima uguaglianza per α e portando tutto a primo membro otteniamo

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

cioè il polinomio non nullo

$$p(x) = \sum_{i=0}^{n-1} a_i x^{i+1} - 1 \in \mathbb{F}[x]$$

si annulla in α, pertanto α è algebrico su $\mathbb{F}$.

□

Corollario 1.2.24. *Se $\alpha \in \mathbb{K}$ è algebrico su $\mathbb{F}$ allora $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg(f(x))$ con $f \in \mathbb{F}[x]$ polinomio minimo di α in $\mathbb{F}$. In altri termini, ogni estensione semplice tramite un elemento algebrico è finita.*

Dimostrazione. Basta osservare che, se $n = \deg(f)$, l'insieme $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forma una base di $\mathbb{F}(\alpha)$ in $\mathbb{F}$. Infatti se per assurdo gli elementi $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ fossero linearmente dipendenti sarebbe possibile trovare un polinomio g di grado minore o uguale a $n-1$ che abbia α come radice, contro la minimalità del grado di f. Inoltre essi generano tutto $\mathbb{F}(\alpha)$ per il teorema precedente. □

Corollario 1.2.25. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Se $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ sono algebrici su $\mathbb{F}$ allora*

$$[\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{F}] \leq \prod_{i=1}^{n} d_i$$

con $d_i = \deg(f_i(x))$ dove $f_i(x)$ è il polinomio minimo di α_i in $\mathbb{F}$.

Dimostrazione. Osserviamo che

$$\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_i)(\alpha_{i+1}) = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_i, \alpha_{i+1})$$

dal momento che se α_i è algebrico su $\mathbb{F}$ lo è anche su $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ la seguente catena di estensioni

$$\mathbb{F} \subseteq \mathbb{F}(\alpha_1) \subseteq \ldots \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_{n-2}) \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$$

è una catane di estensioni finite, da cui

$$[\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{F}] = \prod_{i=1}^{n} [\mathbb{F}(\alpha_1, \ldots, \alpha_i) : \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})].$$

Osserviamo adesso che, detto $p_i(x) \in \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})[x]$ il polinomio minimo di α_i in $\mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})$, abbiamo che $(p_i(x)) = \ker \phi_{\alpha_i}$, quindi dal momento che $f_i \in \mathbb{F}[x] \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})[x]$ e $f_i(\alpha_i) = 0$ deve aversi $f_i \in (p_i(x))$ quindi $p_i | f$, ciò implica che $\deg(p_i) \leq \deg(f_i) = d_i$. Dal corollario precedente abbiamo $[\mathbb{F}(\alpha_1, \ldots, \alpha_i) : \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})] = \deg(p_i) \leq d_i$, pertanto

$$[\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{F}] \leq \prod_{i=1}^{n} d_i$$

□

Corollario 1.2.26. *Un'estensione di campi $\mathbb{F} \subseteq \mathbb{K}$ è finitamente generata e algebrica se e solo se è finita.*

Dimostrazione.

- $\Rightarrow$ Per ipotesi $\mathbb{F} \subseteq \mathbb{K}$ è f.g. quindi devono esistere $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ tali che $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}$. $\mathbb{F} \subseteq \mathbb{K}$ è algebrica, pertanto $\alpha_1, \alpha_2, \ldots, \alpha_n$ saranno algebrici su $\mathbb{F}$, allora in base al corollario precedente l'estensione $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}$ è finita.

- $\Leftarrow$ Già dimostrato nei risultati precedenti.

□

Proposizione-Definizione 1.2.27. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Gli elementi di $\mathbb{K}$ algebrici su $\mathbb{F}$ formano un campo detto* ***chiusura algebrica di $\mathbb{F}$ in $\mathbb{K}$***

Dimostrazione. Siano $\alpha, \beta \in \mathbb{K}$ algebrici su $\mathbb{F}$, per un corollario precedente l'estensione $\mathbb{F} \subseteq \mathbb{F}(\alpha, \beta)$ è finita quindi anche algebrica. Dunque gli elementi $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ sono tutti algebrici su $\mathbb{F}$, questo prova che gli elementi di $\mathbb{K}$ algebrici su $\mathbb{F}$ formano un campo. □

Corollario 1.2.28. *Se $\mathbb{F}, \mathbb{K}$ e $\mathbb{E}$ sono tre campi tali che $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ allora l'estensione $\mathbb{F} \subseteq \mathbb{E}$ è algebrica se e solo se lo sono $\mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{E}$*

Dimostrazione.

- $\Rightarrow$ È ovvio che, essendo $\mathbb{K} \subseteq \mathbb{E}$, se l'estensione $\mathbb{F} \subseteq \mathbb{E}$ è algebrica allora lo è anche $\mathbb{F} \subseteq \mathbb{K}$.
  Sia $\alpha \in \mathbb{E}$, per ipotesi $\exists f \in \mathbb{F}[x] \setminus \{\underline{0}\} : f(\alpha) = 0$, ma essendo $\mathbb{F} \subseteq \mathbb{K}$ si ha $f \in \mathbb{F}[x] \subseteq \mathbb{K}[x]$, quindi α è algebrico su $\mathbb{K}$. Questo prova che $\mathbb{K} \subseteq \mathbb{E}$ è algebrica.

- $\Leftarrow$ Sia $\alpha \in \mathbb{E}$, per ipotesi

  $$\exists f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{K}[x] \setminus \{\underline{0}\} : f(\alpha) = 0.$$

  L'estensione $\mathbb{F} \subseteq \mathbb{F}(a_0, a_1, \ldots, a_n)$ è algebrica poiché ognuno degli $a_i \in \mathbb{K}$ è algebrico su $\mathbb{F}$ per ipotesi. Dal momento che $f \in \mathbb{F}(a_0, \ldots, a_n)[x]$ allora α è algebrico su $\mathbb{F}(a_0, \ldots, a_n)$. Consideriamo adesso le estensioni

  $$\mathbb{F} \subseteq \mathbb{F}(a_0, \ldots, a_n) \subseteq \mathbb{F}(a_0, \ldots, a_n, \alpha)$$

  ognuna di esse è algebrica in quanto α è algebrico su $\mathbb{F}(a_0, \ldots, a_n)$, quindi l'estensione $\mathbb{F} \subseteq \mathbb{F}(a_0, \ldots, a_n, \alpha)$ è algebrica, in particolare α è algebrico su $\mathbb{F}$. Questo prova che l'estensione $\mathbb{F} \subseteq \mathbb{E}$ è algebrica.

□

Teorema 1.2.29. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Se $\alpha \in \mathbb{K}$ è trascendente su $\mathbb{F}$ allora $\mathbb{F}(\alpha) \simeq \mathbb{F}(x)$.*

Dimostrazione. Sia $\phi : \mathbb{F}(x) \to \mathbb{F}(\alpha)$ con

$$\phi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)} \quad \forall f, g \in \mathbb{F}[x], g \neq \underline{0}.$$

È facile verificare che ϕ è un omomorfismo di anelli. Inoltre ϕ è suriettivo poiché, per una proposizione precedente, si ha

$$\mathbb{F}(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{F}[x], g \neq \underline{0}\right\}.$$

Verifichiamo che ϕ è iniettivo. Abbiamo che

$$\frac{f(x)}{g(x)} \in \ker\phi \Leftrightarrow \frac{f(\alpha)}{g(\alpha)} = 0 \Leftrightarrow f(\alpha) = 0 \Leftrightarrow f = \underline{0}$$

(l'ultima equivalenza è vera per la trascendenza di α su $\mathbb{F}$), da cui $\ker\phi = \{\underline{0}\}$, cioè ϕ è iniettivo. Dunque ϕ è un isomorfismo di anelli. □

Lemma 1.2.30. *Se $p(x) \in \mathbb{F}[x]$ è irriducibile con $\deg p(x) = n > 1$ allora esiste un'estensione $\mathbb{F} \subseteq \mathbb{K}$ con $[\mathbb{K} : \mathbb{F}] = n$ nella quale $p(x)$ ha una radice.*

Dimostrazione. Dato che $\mathbb{F}[x]$ è un dominio euclideo e $p(x)$ è irriducibile, l'ideale $I = (p(x))$ è massimale, qundi il quoziente $\mathbb{F}[x]/I$ è un campo.
Consideriamo adesso l'immersione $\varphi : \mathbb{F} \to \mathbb{F}[x]$, la proiezione naturale $\pi : \mathbb{F}[x] \to \mathbb{F}[x]/I$ e infine la composizione $\phi = \pi \circ \varphi : \mathbb{F} \to \mathbb{F}[x]/I$. ϕ è composizione di omomorfismi di anelli quindi è un omomorfismo di anelli, inoltre esso è non banale quindi è iniettivo (se non fosse iniettivo avremo che $\{\underline{0}\} \subsetneq \ker\phi \subsetneq \mathbb{F}$, cioè $\mathbb{F}$ avrebbe un ideale proprio, il che è impossibile poiché $\mathbb{F}$ è un campo), in altri termini ϕ è un'immersione (scriviamo impropriamente $\mathbb{F} \subseteq \mathbb{F}[x]/I$).
Proviamo che

$$p(t) = a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{F}[t]$$

visto come polinomio in $(\mathbb{F}[x]/I)[t]$ ha come radice $\bar{x} = x + I \in \mathbb{F}[x]/I$, infatti

$$p(\bar{x}) = p(x + I) = (a_0 + I) + (a_1 + I)(x + I) + \ldots + (a_n + I)(x + I)^n =$$

$$= (a_0 + a_1 x + \ldots + a_n x^n) + I = p(x) + I = I = 0_{\frac{\mathbb{F}[x]}{I}}.$$

La tesi segue ponendo $\mathbb{K} = \mathbb{F}(\bar{x}) \subseteq \mathbb{F}[x]/I$. □

Osserviamo che $\mathbb{K} = \mathbb{F}(\bar{x}) = \mathbb{F}[\bar{x}] = \mathbb{F}[x]/I$, in quanto $\bar{x}$ è algebrico su $\mathbb{F}$ e $p(x)$ è irriducibile, quindi $(p_{\bar{x}}^{\mathbb{F}}(x)) = (p(x))$.

Proposizione 1.2.31. *Se $f \in \mathbb{F}[x]$ con $\deg f = n$ allora esiste un'estensione $\mathbb{F} \subseteq \mathbb{K}$ in cui f si spezza in fattori lineari. Inoltre $[\mathbb{K} : \mathbb{F}] \leq n!$.*

Dimostrazione. Procediamo per induzione su n.
Se $n = 1$ banalmente $\mathbb{K} = \mathbb{F}$.
Supponiamo il teorema vero fino a $n-1$ e dimostriamolo per n.
Sia $p(x)$ un fattore irriducibile di $f(x)$. Se $\deg p = 1$ allora $f(x) = p(x)q(x)$ con $\deg q = n-1$, per l'ipotesi induttiva $q(x)$ si spezza linearmente in $\mathbb{K}$, quindi anche f dato che p è gia un fattore lineare, inoltre

$$[\mathbb{K} : \mathbb{F}] \leq (n-1)! < n!$$

e questo prova l'asserto.
Supponiamo adesso $\deg p > 1$. Abbiamo $\mathbb{F} \subseteq \mathbb{F}[x]/(p(x)) = \mathbb{E}$. Dal lemma precedente sappiamo che $p(x)$ ha come radice $\bar{x} = x + (p(x))$. Applicando il teorema di Ruffini in $\mathbb{E}[x]$ otteniamo $p(x) = (x - \bar{x})q(x)$ per qualche $q \in \mathbb{E}[x]$. Dal fatto che $p(x)|f(x)$ abbiamo che $f(x) = p(x)h(x) = (x-\bar{x})q(x)h(x)$, per qualche $h \in \mathbb{F}[x] \subseteq \mathbb{E}[x]$, con $\deg q \cdot h = n-1$. Per l'ipotesi induttiva applicata al polinomio $q \cdot h$ (sul campo $\mathbb{E}$) esiste un'estensione $\mathbb{E} \subseteq \mathbb{K}$ in cui $q(x)h(x)$ si spezza in fattori lineari e $[\mathbb{K} : \mathbb{E}] \leq (n-1)!$. Dunque $f(x) = (x-\bar{x})q(x)h(x)$ si spezza linearmente in $\mathbb{K}$, inoltre, poiché $\deg p \leq n$ e $\mathbb{E} = \mathbb{F}(\bar{x})$ si ha $[\mathbb{E} : \mathbb{F}] \leq n$, quindi

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{F}] \leq (n-1)! \cdot n = n!.$$

□

Definizione 1.2.32. *Sia $f \in \mathbb{F}[x]$ con $\deg f(x) \geq 1$, un campo $\mathbb{K} \supseteq \mathbb{F}$ si dice* ***campo di spezzamento di f su $\mathbb{F}$*** *se*

1. *f si spezza in fattori lineari in $\mathbb{K}[x]$ ($\Leftrightarrow$ f ha tutte le radici in $\mathbb{K}$).*
2. *Se $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ sono le radici distinte di f allora $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.*

Osservazione 1.2.33. *Dalla proposizione precedente segue che se $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ è il campo di spezzamento di $f \in \mathbb{F}[x]$ su $\mathbb{F}$ allora l'estensione $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ è finita (oppure, più semplicemente, osservando che ognugno degli α_i è algebrico su $\mathbb{F}$).*

Teorema 1.2.34. *Siano $\mathbb{F}$ e $\mathbb{F}'$ due campi. Supponiamo che esista un isomorfismo $\psi : \mathbb{F} \to \mathbb{F}'$, allora ψ induce un isomorfismo di anelli $\tilde{\psi} : \mathbb{F}[x] \to \mathbb{F}'[x]$ dove*

$$\text{Se } f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x] \text{ allora } \tilde{\psi}(f(x)) = \sum_{i=0}^{n} \psi(a_i) x^i \in \mathbb{F}'[x].$$

Sia adesso $f \in \mathbb{F}[x]$ un polinomio e $f' = \tilde{\psi}(f) \in \mathbb{F}'[x]$. Se $\mathbb{K}$ è il campo di spezzamento di f su $\mathbb{F}$ e $\mathbb{K}'$ sia il campo di spezzamento di f' su $\mathbb{F}'$ allora esiste $\phi : \mathbb{K} \to \mathbb{K}'$ isomorfismo tale che $\phi_{|\mathbb{F}} = \psi$.

Dimostrazione. Sia $\deg f = n$, pertanto $[\mathbb{K} : \mathbb{F}] = m \leq n!$. Procediamo per induzione su m.
Se $m = 1$ banalmente $\phi = \psi$.
Supponiamo il teorema vero fino a $m-1$, dimostriamolo per m. Sia $[\mathbb{K} : \mathbb{F}] = m > 1$ e $p(x)$ un fattore irriducibile di $f(x)$ con $\deg p(x) = r > 1$. Essendo $\mathbb{K}$ campo di spezzamento

di $f(x)$ e $p(x)|f(x)$ allora tutte le radici di $p(x)$ stanno in $\mathbb{K}$. Sia $\alpha \in \mathbb{K}$ una radice di $p(x)$ allora

$$\mathbb{F} \subseteq \mathbb{F}[\alpha] = \mathbb{F}(\alpha) = \frac{\mathbb{F}[x]}{(p(x))}.$$

Sia $p'(x) = \tilde{\psi}(p(x)) \in \mathbb{F}'[x]$, $p'(x)$ è irriducibile in $\mathbb{F}'[x]$, come prima $\mathbb{K}'$ contiene tutte le radici di $p'(x)$. Sia $\alpha' \in \mathbb{K}'$ una radice di $p'(x)$, allora come prima

$$\mathbb{F}' \subseteq \mathbb{F}'[\alpha'] = \mathbb{F}'(\alpha') = \frac{\mathbb{F}'[x]}{(p'(x))}.$$

Consideriamo adesso la proiezione naturale $\pi' : \mathbb{F}'[x] \to \mathbb{F}'[x]/(p'(x))$. La composizione $\pi' \circ \tilde{\psi} : \mathbb{F}[x] \to \mathbb{F}'[x]/(p'(x))$ risulterà un omomorfismo di anelli suriettivo (poiché entrambi $\tilde{\psi}$ e π' sono omomorfismi suriettivi), inoltre

$$\ker(\pi' \circ \tilde{\psi}) = \big\{g \in \mathbb{F}[x] : \tilde{\psi}(g(x)) + (p'(x)) = (p'(x))\big\} = \big\{g \in \mathbb{F}[x] : \tilde{\psi}(g(x)) \in (p'(x))\big\} = (p(x))$$

per il primo teorema dell'isomorfismo esiste un isomorfismo $\tau : \mathbb{F}[\alpha] \to \mathbb{F}'[\alpha']$ con

$$\tau\big(g(x) + (p(x))\big) = \psi(g(x)) + (p'(x)) \quad \forall g \in \mathbb{F}[x] \Longrightarrow \tau_{|\mathbb{F}} = \psi$$

$$\begin{array}{ccc} \mathbb{F}[x] & \xrightarrow{\pi' \circ \tilde{\psi}} & \mathbb{F}'[x]/(p'(x)) \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\tau} & \\ & \mathbb{F}[x]/(p(x)) & \end{array}$$

$\Big($ricordiamo che $\dfrac{\mathbb{F}[x]}{(p(x))} = \mathbb{F}[\alpha], \dfrac{\mathbb{F}'[x]}{(p'(x))} = \mathbb{F}[\alpha']$ $\Big)$.
Inoltre abbiamo che $[\mathbb{F}[\alpha] : \mathbb{F}] = \deg p(x) = r > 1, [\mathbb{K} : \mathbb{F}] = m$ da cui

$$[\mathbb{K} : \mathbb{F}[\alpha]] = \frac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{F}[\alpha] : \mathbb{F}]} = \frac{m}{r} < m.$$

Osserviamo che $f \in \mathbb{F}[x] \subseteq \mathbb{F}(\alpha)[x]$ e $\mathbb{K}$ è campo di spezzamento di f su $\mathbb{F}(\alpha)$, infatti $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n) = \mathbb{F}(\alpha)(\alpha_1, \ldots, \hat{\alpha_i}, \ldots, \alpha_h)$, per lo stesso motivo $\mathbb{K}'$ è campo di spezzamento di f' su $\mathbb{F}'[\alpha']$. Possiamo dunque applicare l'ipotesi induttiva (rispetto ai campi $\mathbb{F}[\alpha]$ e $\mathbb{F}'[\alpha']$) quindi esisterà un isomorfismo $\phi : \mathbb{K} \to \mathbb{K}'$ tale che $\phi_{|\mathbb{F}[\alpha]} = \tau$, ma dal momento che $\tau_{|\mathbb{F}} = \psi$ e $\mathbb{F} \subseteq \mathbb{F}(\alpha)$ avremo che $\phi_{|\mathbb{F}} = \tau_{|\mathbb{F}} = \psi$. Pertanto ϕ è l'isomorfismo cercato. □

Proposizione-Definizione 1.2.35. *Un campo $\mathbb{F}$ è **algebricamente chiuso** se vale almeno una delle seguenti proprietà tra di loro equivalenti*

1. *Ogni polinomio non costante $f \in \mathbb{F}[x] \setminus \mathbb{F}$ ha almeno una radice in $\mathbb{F}$.*
2. *I soli polinomi irriducibili in $\mathbb{F}[x]$ sono quelli di grado 1.*
3. *Ogni polinomio non costante $f \in \mathbb{F}[x] \setminus \mathbb{F}$ si spezza linearmente in $\mathbb{F}[x]$ ($\Leftrightarrow$ f ha tutte le radici in $\mathbb{F}$).*

4. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione algebrica allora $\mathbb{F} = \mathbb{K}$ ($\Leftrightarrow \mathbb{F}$ non ha estensioni algebriche proprie).*

Dimostrazione.

(1) $\Rightarrow$ (2) Sia $f \in \mathbb{F}[x] \setminus \mathbb{F}$, se $\deg f(x) = 1$ allora f è irriducibile, altrimenti se $\deg f(x) > 1$, sia $\alpha \in \mathbb{F}$ una radice di f, per il teorema di Ruffini $f(x) = (x-\alpha)g(x)$ con $\deg g \geq 1$, cioè f è riducibile.

(2) $\Rightarrow$ (3) Basta osservare che essendo $\mathbb{F}[x]$ un UFD ogni polinomio $f \in \mathbb{F}[x] \setminus \mathbb{F}$ è prodotto finito di irriducibili che per ipotesi sono i polinomi di grado 1.

(3) $\Rightarrow$ (4) Sia $\alpha \in \mathbb{K}$, per ipotesi $\exists f \in \mathbb{F}[x] \setminus \mathbb{F} : f(\alpha) = 0$, quindi α è radice di f e pertanto $\alpha \in \mathbb{F}$, questo prova che $\mathbb{K} \subseteq \mathbb{F} \Rightarrow \mathbb{K} = \mathbb{F}$.

(4) $\Rightarrow$ (1) Sia $f \in \mathbb{F}[x] \setminus \mathbb{F}$ e α una radice di f in qualche estensione. L'estensione $\mathbb{F} \subseteq \mathbb{F}(\alpha)$ è algebrica quindi $\mathbb{F} = \mathbb{F}(\alpha)$, cioè $\alpha \in \mathbb{F}$.

□

Dalla (3) della precedente proposizione segue che un campo algebricamente chiuso $\mathbb{F}$ è campo di spezzamento di ogni polinomio $f \in \mathbb{F}[x]$.

Definizione 1.2.36. *Una estensione $\mathbb{F} \subseteq \overline{\mathbb{F}}$ si dice **chisura algebrica** di $\mathbb{F}$ se*

1. *$\mathbb{F} \subseteq \overline{\mathbb{F}}$ è algebrica.*
2. *$\overline{\mathbb{F}}$ è algebricamente chiuso.*

Proposizione 1.2.37. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione algebrica. Se ogni polinomio $f \in \mathbb{F}[x]$ si spezza linearmente in $\mathbb{K}[x]$ allora $\mathbb{K}$ è una chiusura algebrica di $\mathbb{F}$.*

Dimostrazione. Per ipotesi $\mathbb{F} \subseteq \mathbb{K}$ è algebrica, basta quindi dimostrare che $\mathbb{K}$ è algebricamente chiuso. Sia $\mathbb{K} \subseteq \mathbb{E}$ un'estensione algebrica e sia $\alpha \in \mathbb{E}$. α è algebrico su $\mathbb{F}$ quindi per ipotesi il suo polinomio minimo in $\mathbb{F}$ si spezza linearmente in $\mathbb{K}[x]$ da cui $\alpha \in \mathbb{K}$, cioè $\mathbb{E} = \mathbb{K}$ da cui $\mathbb{K}$ è algebricamente chiuso. □

Teorema 1.2.38. *Se $\mathbb{F}$ è un campo allora*

1. *Esiste una chiusura algebrica di $\mathbb{F}$ (che indicheremo con $\overline{\mathbb{F}}$).*
2. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione algebrica allora esiste $\phi : \mathbb{K} \to \overline{\mathbb{F}}$ omomorfismo iniettivo tale che $\phi_{|\mathbb{F}} = 1_{\mathbb{F}}$.*
3. *Due chiusure algebriche sono isomorfe mediante un isomorfismo che lascia fisso $\mathbb{F}$.*

Dimostrazione.

1. Sia $\Sigma = \{\mathbb{K} \text{ campo} : \mathbb{F} \subseteq \mathbb{K} \text{ algebrica}\}$. Osserviamo che $\mathbb{F} \in \Sigma \neq \emptyset$, Σ rispetto alla relazione $\subseteq$ è un insieme parzialmente ordinato, infine ogni catena $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \ldots \subseteq \mathbb{K}_n \subseteq \ldots$ in Σ ammette maggiorante $\bigcup_i \mathbb{K}_i$. Siamo nelle ipotesi del lemma di Zorn quindi esiste $\overline{\mathbb{F}} \in \Sigma$ massimale, quindi $\overline{\mathbb{F}}$ risulterà algebricamente chiuso per definizione. Inoltre, essendo $\mathbb{F} \subseteq \overline{\mathbb{F}}$ algebrica, $\overline{\mathbb{F}}$ risulterà una chiusura algebrica di $\mathbb{F}$.

2. Omessa

3. Siano $\mathbb{K}$ e $\overline{\mathbb{F}}$ due chiusure algebriche di $\mathbb{F}$. Dal punto (2) esiste un omomorfismo $\phi : \mathbb{K} \to \overline{\mathbb{F}}$ tale che $\phi_{|\mathbb{F}} = 1_{\mathbb{F}}$. Dunque $\mathbb{F} \subseteq \mathbb{K} \simeq \phi(\mathbb{K}) \subseteq \overline{\mathbb{F}}$, inoltre considerando che $\mathbb{F} \subseteq \overline{\mathbb{F}}$ è algebrica si ha $\phi(\mathbb{K}) = \overline{\mathbb{F}}$.

□

Dal precedente teorema segue che la chiusura algebrica di un campo $\mathbb{K}$ (che indicheremo con $\overline{\mathbb{K}}$) è unica a meno di isomorfismi.

Corollario 1.2.39. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione algebrica allora $\overline{\mathbb{F}} \simeq \overline{\mathbb{K}}$.*

Dimostrazione. L'estensione $\mathbb{F} \subseteq \overline{\mathbb{K}}$ è algebrica quindi esiste un omomorfismo iniettivo $\phi : \overline{\mathbb{K}} \to \overline{\mathbb{F}}$ tale che $\phi_{|\mathbb{F}} = 1_{\mathbb{F}}$. Poiché $\mathbb{F} \subseteq \overline{\mathbb{K}} \simeq \phi(\overline{\mathbb{K}}) \subseteq \overline{\mathbb{F}}$, essendo $\overline{\mathbb{K}} \simeq \phi(\overline{\mathbb{K}}) \subseteq \overline{\mathbb{F}}$ un'estensione algebrica e $\overline{\mathbb{K}}$ algebricamente chiuso si ha $\overline{\mathbb{K}} \simeq \phi(\overline{\mathbb{K}}) = \overline{\mathbb{F}}$. □

L'insieme $\overline{\mathbb{Q}}$ è detto **campo dei numeri algebrici**. Osserviamo che si ha $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, infatti se per assurdo $[\overline{\mathbb{Q}} : \mathbb{Q}] = n$ allora essendo il polinomio minimo di $\sqrt[n+1]{2}$ in $\mathbb{Q}$ uguale a $x^{n+1} - 2 \in \mathbb{Q}[x]$ abbiamo che $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[n+1]{2}] \subseteq \overline{\mathbb{Q}}$ con $[\mathbb{Q}[\sqrt[n+1]{2}] : \mathbb{Q}] = n + 1$, assurdo.

1.3 Campi finiti

Definizione 1.3.1. *Un campo $\mathbb{K}$ si dice **finito** se $|\mathbb{K}| < \infty$, **infinito** se non è finito.*

Osservazione 1.3.2. *Se un campo $\mathbb{K}$ è finito allora necessariamente $ch(\mathbb{K}) > 0$, altrimenti se fosse $ch(\mathbb{K}) = 0$ si avrebbe $\mathbb{Q} \subseteq \mathbb{K}$ con $|\mathbb{Q}| = \infty$, contro il fatto che $\mathbb{K}$ è finito.*

Proposizione 1.3.3. *Se $\mathbb{K}$ è un campo finito allora $|\mathbb{K}| = p^m$ con $p = ch(\mathbb{K})$ e $m \in \mathbb{N} \setminus \{0\}$.*

Dimostrazione. Per quanto finora dimostrato deve aversi $ch(\mathbb{K}) = p$ con p primo. Dunque $\mathbb{Z}_p \subseteq \mathbb{K}$ e pertanto $\mathbb{K}$ è uno spazio vettoriale su $\mathbb{Z}_p$. Essendo $|\mathbb{K}| < \infty$ allora esiste un insieme finito di generatori di $\mathbb{K}$ (come spazio vettoriale) quindi $\dim_{\mathbb{Z}_p} \mathbb{K} = m$, da cui $\mathbb{K} \simeq \mathbb{Z}_p^m$ cioè $|\mathbb{K}| = |\mathbb{Z}_p^m| = p^m$. □

Proposizione 1.3.4. *Se $\mathbb{K}$ è un campo finito con $|\mathbb{K}| = p^m$ allora $\mathbb{K}$ è campo di spezzamento del polinomio $x^{p^m} - x \in \mathbb{Z}_p[x]$.*

Dimostrazione. $(\mathbb{K}^*, \cdot)$ è un gruppo abeliano finito ($\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$), dal teorema di Lagrange sappiamo che

$$\forall a \in \mathbb{K}^* \quad a^{o(\mathbb{K}^*)} = 1_{\mathbb{K}} \quad \text{con } o(\mathbb{K}^*) = p^m - 1$$

quindi

$$a^{p^m - 1} = 1_{\mathbb{K}} \Rightarrow a^{p^m} = a \Rightarrow a^{p^m} - a = 0,$$

cioè ogni elemento di $\mathbb{K}$ è radice del polinomio $x^{p^m} - x \in \mathbb{Z}_p[x]$. Ma $x^{p^m} - x$ ha al più p^m radici, pertanto $\mathbb{K}$ è costituito da tutte e sole le radici di $x^{p^m} - x$ e quindi $x^{p^m} - x$ si spezza linearmente in $\mathbb{K}$. □

Teorema 1.3.5. *Sia p un numero primo. Per ogni $m \in \mathbb{N} \setminus \{0\}$ esiste un campo $\mathbb{K}$ tale che $|\mathbb{K}| = p^m$, inoltre due campi con p^m elementi sono tra loro isomorfi.*

Dimostrazione. Consideriamo il polinomio $x^{p^m} - x \in \mathbb{Z}_p[x]$ e sia $\mathbb{L}$ il suo campo di spezzamento. L'estensione $\mathbb{Z}_p \subseteq \mathbb{L}$ è finita, in quanto $\mathbb{L} = \mathbb{Z}_p(\alpha_1, \alpha_2, \ldots, \alpha_h)$ con α_i radici di $x^{p^m} - x$, dunque $|\mathbb{L}| < \infty$. Sia $\mathbb{K} = \{\alpha \in \mathbb{L} : \alpha^{p^m} - \alpha = 0\} \subseteq \mathbb{L}$, proviamo che $\mathbb{K}$ è un campo. Siano $a, b \in \mathbb{K}^*$ allora

$$(ab)^{p^m} = a^{p^m} b^{p^m} = ab \neq 0 \Rightarrow ab \in \mathbb{K}^*,$$

questo prova che $(\mathbb{K}^*, \cdot)$ è un sottogruppo di $(\mathbb{L}^*, \cdot)$ (ricordiamo che $\mathbb{L}^*$ è finito); inoltre, dato che $\mathbb{L}$ ha caratteristica p e $\mathbb{K} \subseteq \mathbb{L}$, dal lemma (1.1.6) abbiamo che

$$(a + b)^p = a^p + b^p$$

quindi, applicando ripetutamente la precedente formula si ha

$$(a + b)^{p^m} = a^{p^m} + b^{p^m} = a + b \Rightarrow a + b \in \mathbb{K}$$

e questo prova che $(\mathbb{K}, +)$ è un sottogruppo di $(\mathbb{L}, +)$ da cui $\mathbb{K}$ è un sottocampo di $\mathbb{L}$. Inoltre essendo $\mathbb{L}$ il campo di spezzamento di $x^{p^m} - x$ esso è il più piccolo campo contenente tutte le radici di $x^{p^m} - x$ pertanto $\mathbb{L} = \mathbb{K}$. Inoltre, dato che $D(x^{p^m} - x) = p^m x^{p^m - 1} - 1 = -1 \neq 0 \quad \forall x \in \mathbb{K}$, allora $x^{p^m} - x$ non ha radici multiple quindi le sue radici sono tutte distinte, dunque $|\mathbb{K}| = p^m$.
Inoltre se $\mathbb{F}$ è un campo con $|\mathbb{F}| = p^m$ allora $\mathbb{F}$ è campo di spezzamento di $x^{p^m} - x \in \mathbb{Z}_p[x]$, quindi $\mathbb{F} \simeq \mathbb{K}$. □

Lemma 1.3.6. *Sia G un gruppo abeliano finito. Se $a, b \in G$ allora esiste $c \in G$ tale che $o(c) = m.c.m.(o(a), o(b))$.*

(segue dal teorema di struttura dei gruppi abeliani finiti)

Proposizione 1.3.7. *Se $\mathbb{K}$ è un campo finito allora $(\mathbb{K}^*, \cdot)$ è un gruppo ciclico.*

Dimostrazione. Dal momento che $\mathbb{K}$ è un campo finito allora $|\mathbb{K}| = p^m$. Sia $h = p^m - 1 = |\mathbb{K}^*|$ e $n = m.c.m.(o(a) : a \in \mathbb{K}^*)$, applicando il precedente lemma ricorsivamente sappiamo che esiste $c \in \mathbb{K}^* : o(c) = n$. Dal teorema di Lagrange sappiamo che $n = o(c) \mid h = |\mathbb{K}^*|$, in particolare $n \leq h$. Il polinomio $x^n - 1$ ha al più n radici, poiché $\forall a \in \mathbb{K}^* \quad a^n = 1$ in quanto $n = m.c.m.(o(a) : a \in \mathbb{K}^*)$ allora deve aversi $h \leq n$, da cui $n = h = o(c) = |\mathbb{K}^*|$ quindi $\mathbb{K}^* = \mathcal{G}(c)$. □

1.4 Estensioni separabili

Proposizione 1.4.1. *Sia $f \in \mathbb{F}[x]$. Se $g = MCD(f, f') \in \mathbb{F}[x]$ allora f ha radici multiple se e solo se* $\deg g(x) \geq 1$.

Dimostrazione. f ha radici multiple $\Leftrightarrow \exists a \in \mathbb{K} \supseteq \mathbb{F} : f(a) = f'(a) = 0 \Leftrightarrow (x - a) \mid f, f'$ (in $\mathbb{K}[x]$) $\Leftrightarrow (x - a) \mid g$ (in $\mathbb{K}[x]$) $\Leftrightarrow \deg g(x) \geq 1$. □

Osservazione 1.4.2. *Se $f, g \in \mathbb{F}[x]$ e $\mathbb{F} \subseteq \mathbb{K}$ allora $MCD(f, g)$ è indipendente dal campo in cui viene calcolato in quanto si ottiene con l'algoritmo euclideo che lavora con i coefficienti di f e g, quindi in ogni caso $MCD(f, g) \in \mathbb{F}[x]$.*

Definizione 1.4.3.

1. *Un polinomio $f \in \mathbb{F}[x]$ si dice* ***separabile*** *nel suo campo di spezzamento se tutte le sue radici sono distinte.*
2. *Sia $\mathbb{F} \subseteq \mathbb{K}$ e $\alpha \in \mathbb{K}$ algebrico su $\mathbb{F}$. α è detto* ***separabile*** *su $\mathbb{F}$ se è tale il suo polinomio minimo in $\mathbb{F}$.*
3. *Un'estensione $\mathbb{F} \subseteq \mathbb{K}$ è detta* ***separabile*** *se ogni $\alpha \in \mathbb{K}$ è separabile su $\mathbb{F}$.*

Lemma 1.4.4. *Sia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ una catena di estensioni di campi. Se $\mathbb{F} \subseteq \mathbb{K}$ è separabile allora lo sono anche $\mathbb{F} \subseteq \mathbb{L}$ e $\mathbb{L} \subseteq \mathbb{K}$.*

Dimostrazione. Se $\alpha \in \mathbb{L} \subseteq \mathbb{K}$ allora $\alpha \in \mathbb{K}$ quindi α è separabile su $\mathbb{F}$. Questo prova che l'estensione $\mathbb{F} \subseteq \mathbb{L}$ è separabile.
Sia $\alpha \in \mathbb{K}$, α è separabile su $\mathbb{F}$ quindi $p_\alpha^{\mathbb{F}}(x) \in \mathbb{F}[x] \subseteq \mathbb{L}[x]$ ha tutte le radici distinte, inoltre dato che $\mathbb{F} \subseteq \mathbb{L}$ si ha $p_\alpha^{\mathbb{L}}(x) | p_\alpha^{\mathbb{F}}(x)$ quindi anche $p_\alpha^{\mathbb{L}}(x) \in \mathbb{L}[x]$ ha tutte le radici distinte, da cui $\alpha \in \mathbb{K}$ è separabile su $\mathbb{L}$. Ciò prova che l'estensione $\mathbb{L} \subseteq \mathbb{K}$ è separabile. □

Lemma 1.4.5. *Se $f \in \mathbb{F}[x]$ con $\deg f(x) \geq 1$ e $ch(\mathbb{F}) = 0$ allora $f' \neq \underline{0}$.*

Dimostrazione. Dato che $\deg f(x) \geq 1$ allora possiamo scrivere

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

con $a_n \neq 0$. Per assurdo supponiamo che

$$f'(x) = n \cdot a_n x^{n-1} + \ldots + 2 \cdot a_2 x + a_1 = \underline{0}.$$

Poiché $a_n \neq 0$ si ha $n \cdot a_n = a_n(n \cdot 1) = 0 \Rightarrow n \cdot 1 = 0$ contro $ch(\mathbb{F}) = 0$, assurdo. □

Corollario 1.4.6. *Sia $f \in \mathbb{F}[x]$ irriducibile con $\deg f(x) \geq 1$ allora*

1. *Se $ch(\mathbb{F}) = 0$ allora f è separabile.*
2. *Se $ch(\mathbb{F}) = p$ allora f non è separabile $\iff \exists g \in \mathbb{F}[x] : f(x) = g(x^p)$.*

Dimostrazione.

1. Dal lemma precedente sappiamo che $f' \neq \underline{0}$, inoltre dal momento che $\deg f'(x) < \deg f(x)$ con f irriducibile allora necessariamente $MCD(f, f') = 1$, cioè f non ha radici multiple quindi è separabile.
2. Se $f' \neq \underline{0}$ allora analogamente al punto precedente f è separabile. Se $f' = \underline{0}$ allora $MCD(f, f') = f$ con $\deg f(x) \geq 1$ quindi f ha radici multiple, cioè f non è separabile. Così facendo abbiamo dimostrato che

   $$f \text{ non è separabile } \iff f' = \underline{0}.$$

   Adesso basta provare che

   $$f' = \underline{0} \iff \exists g \in \mathbb{F}[x] : f(x) = g(x^p).$$

$\Rightarrow$ Supponiamo

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

allora

$$f'(x) = n \cdot a_n x^{n-1} + \ldots + 2 \cdot a_2 x + a_1 = \underline{0}$$

da cui $i \cdot a_i = a_i(i \cdot 1) = 0$. Poiché $ch(\mathbb{F}) = p$ allora se $p \nmid i$ deve aversi $a_i = 0$, pertanto

$$f(x) = a_{ph} x^{ph} + \ldots + a_{2p} x^{2p} + a_p x^p + a_0$$

dove $h \in \mathbb{N}$ è tale che $ph \leq n < p(h+1)$. Ponendo

$$g(x) = a_{ph} x^h + \ldots + a_{2p} x^2 + a_p x + a_0$$

otteniamo $f(x) = g(x^p)$.

$\Leftarrow$ Banale dato che $ch(\mathbb{F}) = p$.

□

Corollario 1.4.7. *Se $\mathbb{F}$ è un campo con $ch(\mathbb{F}) = 0$, allora ogni estensione $\mathbb{F} \subseteq \mathbb{K}$ algebrica è anche separabile.*

Dimostrazione. Basta osservare che ogni elemento $\alpha \in \mathbb{K}$ algebrico su $\mathbb{F}$ risulta separabile in quanto il suo polinomio minimo per definizione è irriducibile, quindi in base al risultato precedente esso è separabile. □

Proposizione 1.4.8. *Se $\mathbb{F}$ è un campo finito allora ogni estensione $\mathbb{F} \subseteq \mathbb{K}$ algebrica è separabile.*

Dimostrazione. Sia $\alpha \in \mathbb{K}$ e $p(x) \in \mathbb{F}[x]$ il suo polinomio minimo in $\mathbb{F}$. L'estensione $\mathbb{F} \subseteq \mathbb{F}(\alpha)$ è finita in quanto α è algebrico su $\mathbb{F}$, quindi $|\mathbb{F}(\alpha)| < \infty$ cioè $|\mathbb{F}(\alpha)| = p^m$. In questo modo $\mathbb{F}(\alpha)$ è campo di spezzamento di $x^{p^m} - x$, inoltre $D(x^{p^m} - x) = -1$ pertanto $x^{p^m} - x$ non ha radici multiple, ma $\alpha \in \mathbb{F}(\alpha)$ è radice di $x^{p^m} - x$ dunque, se $p(x)$ è il polinomio minimo di α su $\mathbb{F}$ allora $p(x) \mid x^{p^m} - x$, in particolare $p(x)$ ha tutte le radici distinte, cioè α è separabile. Ciò prova che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è separabile. □

Dai risultati precedenti si nota facilmente che il concetto di separabilità è significativo nel caso in cui $\mathbb{F}$ è infinito e $ch(\mathbb{F}) > 0$.

Vediamo adesso un esempio di estensione non separabile.

Esempio 1.4.9. *Sia t un'indeterminata su $\mathbb{Z}_p$ e $u = t^p$ con p primo. Poniamo $\mathbb{K} = \mathbb{Z}_p(t)$ e $\mathbb{F} = \mathbb{Z}_p(u)$, si ha*

$$\mathbb{F} = \mathbb{Z}_p(u) = \mathbb{Z}_p(t^p) \subseteq \mathbb{Z}_p(t) = \mathbb{K}.$$

Osserviamo che u è trascendente su $\mathbb{Z}_p$, infatti se per assurdo u fosse algebrico esisterebbe $f \in \mathbb{Z}_p[x] \setminus \{\underline{0}\} : f(u) = 0 \Leftrightarrow f(t^p) = 0$ contro il fatto che t è un'indeterminata su $\mathbb{Z}_p$. Questo prova anche che u è irriducibile in $\mathbb{Z}_p[u]$ (infatti se u fosse algebrico su $\mathbb{Z}_p$ allora $\mathbb{Z}_p[u] = \mathbb{Z}_p(u)$ quindi u sarebbe un invertibile di $\mathbb{Z}_p[u]$).
Il polinomio $x^p - u \in (\mathbb{Z}_p[u])[x]$ è irriducibile per il criterio di Eisenstein (è un polinomio primitivo e u è primo in $\mathbb{Z}_p[u]$, in quanto essendo $\mathbb{Z}_p[u]$ dominio euclideo ogni

elemento irriducibile è primo) quindi, applicando il lemma di Gauss, è irriducibile anche in $\mathbb{Z}_p(u)[x] = \mathbb{F}[x]$. *Poiché*

$$(x^p - u)(t) = t^p - t^p = 0,$$

t *è una radice del polinomio* $x^p - u$ *ed essendo tale polinomio monico e irriducibile allora esso è il polinomio minimo di* t *in* $\mathbb{F}$. *Osserviamo infine che* $x^p - u$ *si fattorizza in* $\mathbb{K}[x]$ *come segue*

$$x^p - u = x^p - t^p = (x - t)^p$$

quindi $x^p - u$ *ha una sola radice di molteplicità* p, *pertanto* t *non è separabile e di conseguenza l'estensione algebrica*

$$\mathbb{F} \subseteq \mathbb{F}(t) = \mathbb{Z}_p(u)(t) = \mathbb{Z}_p(t^p, t) = \mathbb{Z}_p(t) = \mathbb{K} \quad (t \text{ è algebrico su } \mathbb{F})$$

non è separabile.

1.5 Polinomi simmetrici

Definizione 1.5.1. *Si chiamano* ***monomi*** *tutti i polinomi di* $\mathbb{F}[x_1, x_2, \ldots, x_n]$ *del tipo* $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$.
Definiamo il grado del monomio $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ *come il numero*

$$\deg(x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}) = i_1 + i_2 + \ldots + i_n.$$

Sia

$$f(x_1, x_2, \ldots, x_n) = \sum a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in \mathbb{F}[x_1, x_2, \ldots, x_n],$$

definiamo il ***grado del polinomio*** f *come il numero*

$$\deg f = \max\{\deg(x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}) : a_{i_1, i_2, \ldots, i_n} \neq 0\}$$

Utilizziamo la seguente notazione: se $\alpha = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ allora poniamo

$$\underline{x}^{\alpha} = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Sia $\mathcal{M}$ l'insieme di tutti i monomi di $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Vogliamo introdurre su $\mathcal{M}$ un ordinamento totale che soddisfi la proprietà

$$\forall \alpha, \beta, \gamma \in \mathbb{N}^n \quad \underline{x}^{\alpha} \leq \underline{x}^{\beta} \Rightarrow \underline{x}^{\alpha+\gamma} \leq \underline{x}^{\beta+\gamma}. \tag{1.1}$$

Definizione 1.5.2. *Si chiama* ***ordinamento lessicografico graduato****, indicato con* $\leq_{deglex}$, *la relazione su* $\mathcal{M}$

$$x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \leq x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \iff \begin{cases} i_1 + \ldots + i_n < j_1 + \ldots + j_n \\ \\ \textit{oppure} \\ \\ i_1 + \ldots + i_n = j_1 + \ldots + j_n \ \textit{e} \ i_1 = j_1, \ldots, i_k = j_k, i_{k+1} < j_{k+1} \end{cases}$$

Si verifica facilmente che $\leq_{\text{deglex}}$ è un ordinamento totale su $\mathcal{M}$ e soddisfa la (1.1).

Definizione 1.5.3. *Sia $f = c_1m_1 + \ldots + c_nm_n \in \mathbb{F}[x_1, \ldots, x_n]$ con $m_i \in \mathcal{M}$ e $c_i \in \mathbb{F} \setminus \{0\}$ e supponiamo che $m_j \leq m_1 \, \forall j \in \{1, \ldots, n\}$. Diamo le seguenti definizioni:*

$$\begin{array}{ll} lm(f) = m_1 & \textbf{\textit{leading monomial}} \\ lc(f) = c_1 & \textbf{\textit{leading coefficient}} \\ lt(f) = c_1m_1 & \textbf{\textit{leading term}} \end{array}$$

Dalla definizione segue subito che se $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ allora

$$\begin{array}{rcl} lm(f \cdot g) & = & lm(f) \cdot lm(g) \\ lc(f \cdot g) & = & lc(f) \cdot lc(g) \\ lt(f \cdot g) & = & lt(f) \cdot lt(g) \end{array}$$

Osservazione 1.5.4. *Fissato un $m \in \mathcal{M}$ esiste un numero finito di monomi più piccoli di m.*

Definizione 1.5.5. *Un polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$* ***simmetrico*** *se*

$$\forall \sigma \in S_n \quad f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Definizione 1.5.6. *I polinomi*

$$\begin{array}{rcl} \sigma_1(x_1, \ldots, x_n) & = & \displaystyle\sum_{i=1}^{n} x_i \\ \sigma_2(x_1, \ldots, x_n) & = & \displaystyle\sum_{1 \leq i < j \leq n} x_ix_j \\ & \vdots & \\ \sigma_k(x_1, \ldots, x_n) & = & \displaystyle\sum_{1 \leq i_1 < \ldots < i_n \leq n} x_{i_1} \ldots x_{i_n} \\ & \vdots & \\ \sigma_n(x_1, \ldots, x_n) & = & \displaystyle\prod_{i=1}^{n} x_i \end{array}$$

sono detti ***polinomi simmetrici elementari****.*

Osserviamo che i polinomi simmetrici elementari sono tutti simmetrici, infatti se consideriamo il polinomio

$$g(x_1, \ldots, x_n, x) = (x - x_1)(x - x_2) \ldots (x - x_n) = \prod_{i=1}^{n} (x - x_i) \in \mathbb{F}[x_1, x_2, \ldots, x_n][x]$$

ponendo $\sigma_0(x_1, \ldots, x_n) = 1$, si ha

$$g(x_1, \ldots, x_n, x) = \sum_{i=0}^{n} (-1)^i \sigma_i(x_1, \ldots, x_n) x^{n-i}$$

poiché ovviamente

$$\forall \sigma \in S_n \quad g(x_1, \ldots, x_n, x) = \prod_{i=1}^{n}(x - x_i) = \prod_{i=1}^{n}(x - x_{\sigma(i)}) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}, x)$$

dal principio di identità dei polinomi otteniamo che

$$\forall \sigma \in S_n \quad \sigma_i(x_1, \ldots, x_n) = \sigma_i(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \quad \forall i \in \{1, \ldots, n\}.$$

Teorema 1.5.7. (Teorema fondamentale sui polinomi simmetrici) *Ogni polinomio simmetrico di $\mathbb{F}[x_1, x_2, \ldots, x_n]$ si scrive in modo unico come un polinomio a coefficienti in $\mathbb{F}$ nelle variabili di polinomi simmetrici elementari.*

Dimostrazione. (dimostriamo solo l'esistenza) Sia $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ un polinomio simmetrico e sia $lt(f) = \alpha x_1^{h_1} x_2^{h_2} \ldots x_n^{h_n}$. Proviamo che $h_n \leq h_{n-1} \leq \ldots \leq h_1$. Per assurdo supponiamo che $\exists i \in \{1, \ldots, n\} : h_{i+1} > h_i$, allora, dato che f è simmetrico, considerando la permutazione $\sigma = \begin{pmatrix} i & i+1 \end{pmatrix} \in S_n$ otteniamo che il monomio $\alpha x_1^{h_1} \ldots x_i^{h_{i+1}} x_{i+1}^{h_i} \ldots x_n^{h_n}$ dev'essere un monomio di f, ma

$$x_1^{h_1} \ldots x_i^{h_i} x_{i+1}^{h_{i+1}} \ldots x_{h_n}^{n} < x_1^{h_1} \ldots x_i^{h_{i+1}} x_{i+1}^{h_i} \ldots x_{h_n}^{n}$$

contro il fatto che $lt(f) = x_1^{h_1} \ldots x_i^{h_i} x_{i+1}^{h_{i+1}} \ldots x_{h_n}^{n}$, assurdo. In questo modo si ha

$$h_1 - h_2 \geq 0, \ldots, h_{n-1} - h_n \geq 0,$$

quindi possiamo considerare il polinomio $g_1 = \alpha \sigma_1^{h_1 - h_2} \sigma_2^{h_2 - h_3} \ldots \sigma_{n-1}^{h_{n-1} - h_n} \sigma_n^{h_n}$: Ricordando le proprietà del leading term abbiamo

$$lt(g_1) = \alpha x_1^{h_1 - h_2} (x_1 x_2)^{h_2 - h_3} \ldots (x_1 \ldots x_n)^{h_n} = \alpha x_1^{h_1} \ldots x_n^{h_n} = lt(f)$$

quindi $lt(f - g_1) < lt(f)$. Adesso ci sono due possiblità: se $lt(f - g_1) = \beta \in \mathbb{F}$ allora $f = g_1 + \beta \in \mathbb{F}[\sigma_1, \ldots, \sigma_n]$ e si ha la tesi, altrimenti, dato che i monomi piu piccoli di $lt(f)$ sono in numero finito, reiteriamo il procedimento sul polinomio $f - g_1$. Così facendo dopo un numero finito k di passi dovremmo ottenerene

$$f = g_1 + g_2 + \ldots + g_k + \beta \in \mathbb{F}[\sigma_1, \ldots, \sigma_n] \qquad \square.$$

Corollario 1.5.8. *Sia $f(x) \in \mathbb{F}[x]$ un polinomio monico con $\deg f \geq 1$ e siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ tutte le sue radici in qualche estensione $\mathbb{K} \supseteq \mathbb{F}$. Se $p(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ è un polinomio simmetrico allora $p(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}$.*

Dimostrazione. Dal teorema fondamentale sui polinomi simmetrici sappiamo che esiste $\tilde{p} \in \mathbb{F}[x_1, \ldots, x_n]$ tale che

$$p(x_1, \ldots, x_n) = \tilde{p}\big(\sigma_1(x_1, \ldots, x_n), \sigma_2(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\big).$$

Ma scrivendo la fattorizzazione di f

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=0}^{n}(-1)^i \sigma_i(\alpha_1, \ldots, \alpha_n) x^{n-i} \in \mathbb{F}[x]$$

otteniamo $\sigma_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}$ per ogni $i \in \{1, \ldots, n\}$, da cui

$$p(\alpha_1, \ldots, \alpha_n) = \tilde{p}\big(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)\big) \in \mathbb{F} \qquad \square.$$

1.6 Teorema dell'elemento primitivo

Teorema 1.6.1. (Teorema dell'elemento primitivo, versione debole)
Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione finitamente generata e separabile allora esiste $\gamma \in \mathbb{K} : \mathbb{F}(\gamma) = \mathbb{K}$. γ è detto ***elemento primitivo****.*

Dimostrazione. Dividiamo la dimostrazione in due casi.

1. Supponiamo $\mathbb{F}$ finito. Dato che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è finita (poiché finitamente generata e algebrica) allora anche $\mathbb{K}$ risulterà finito. Dunque $(\mathbb{K}^*, \cdot)$ è un gruppo ciclico e pertanto $\mathbb{K} = \mathbb{F}(\gamma)$ per qualche $\gamma \in \mathbb{K}^*$.

2. Supponiamo $\mathbb{F}$ infinito. Per ipotesi $\mathbb{K} = \mathbb{F}(\delta_1, \dots, \delta_n)$, procediamo per induzione su n.

   - Se $n = 1$ il teorema è banale.
   - Se $n = 2$ allora $\mathbb{K} = \mathbb{F}(\alpha, \beta)$ con $\alpha, \beta \in \mathbb{K}$. Sia $p_\alpha(x)$ il polinomio minimo di α in $\mathbb{F}$ e siano $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$ le sue radici (distinte per ipotesi) con $r = \deg p_\alpha$. Analogamente sia $p_\beta(x)$ il polinomio minimo di β in $\mathbb{F}$ e siano $\beta = \beta_1, \beta_2, \dots, \beta_s$ le sue radici (distinte per ipotesi) con $s = \deg p_\beta$. Poniamo

   $$\lambda_{i,j} = \frac{\alpha - \alpha_i}{\beta_j - \beta} \in \mathbb{K} \quad i \in \{1, \dots, r\},\, j \in \{2, \dots, s\}.$$

   Poiché $\mathbb{F}$ è infinito esiste $\lambda \in \mathbb{F}$ tale che $\lambda \neq \lambda_{i,j}\, \forall i \in \{1, \dots, r\}, \forall j \in \{2, \dots, s\}$. Sia $\gamma = \alpha + \lambda\beta \in \mathbb{K}$, abbiamo

   $$(\beta_j - \beta)\lambda \neq \alpha - \alpha_i \Rightarrow \gamma = \alpha + \lambda\beta \neq \alpha_i + \lambda\beta_j.$$

   Adesso consideriamo i due polinomi

   $$h_1(x) = p_\alpha(\gamma - \lambda x) \in \mathbb{F}(\gamma)[x]$$
   $$h_2(x) = p_\beta(x) \in \mathbb{F}[x] \subseteq \mathbb{F}(\gamma)[x].$$

   Il polinomio h_1 ha β come radice, infatti $h_1(\beta) = p_\alpha(\gamma - \lambda\beta) = p_\alpha(\alpha) = 0$, inoltre per ogni $j \in \{2, \dots, s\}$ abbiamo $h_1(\beta_j) \neq 0$, infatti se esistesse un indice $\bar{j} \in \{2, \dots, s\}$ tale che $h_1(\beta_{\bar{j}}) = p_\alpha(\gamma - \lambda\beta_{\bar{j}}) = 0$ allora $\gamma - \lambda\beta_j = \alpha_i$ per qualche $i \in \{1, \dots, r\}$, quindi si avrebbe $\gamma = \alpha + \lambda\beta = \alpha_i + \lambda\beta_j$, assurdo. Dunque si ha

   $$MCD(h_1, h_2) = x - \beta \in \mathbb{F}(\gamma)[x] \Rightarrow \alpha = \gamma - \lambda\beta \in \mathbb{F}(\gamma)$$

   da cui $\mathbb{K} = \mathbb{F}(\alpha, \beta) \subseteq \mathbb{F}(\gamma) \subseteq \mathbb{K} \Rightarrow \mathbb{K} = \mathbb{F}(\gamma)$.

   - Adesso Supponiamo il teorema vero per $m < n$ con $n \geq 3$ e proviamolo per n. Abbiamo

   $$\mathbb{F} \subseteq \mathbb{F}(\delta_1, \delta_2, \dots, \delta_{n-1}) \subseteq \mathbb{F}(\delta_1, \delta_2, \dots, \delta_{n-1}, \delta_n) = \mathbb{K},$$

   per l'ipotesi induttiva $\exists \beta \in \mathbb{F}(\delta_1, \dots, \delta_{n-1})$ tale che $\mathbb{F}(\delta_1, \dots, \delta_{n-1}) = \mathbb{F}(\beta)$, quindi $\mathbb{K} = \mathbb{F}(\beta, \delta_n)$, sempre per l'ipotesi induttiva $\exists \gamma \in \mathbb{K}$ tale che $\mathbb{K} = \mathbb{F}(\gamma)$.

□

Vediamo una generalizzazione del precedente teorema.

Teorema 1.6.2. (Teorema dell'elemento primitivo, versione forte) *Se* $\mathbb{F} \subseteq \mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$ *è un'estensione di campi con* δ_i *separabile su* $\mathbb{F}$ *per ogni* $i \in \{1, \ldots, n\}$ *allora esiste* $\gamma \in \mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$ *separabile su* $\mathbb{F}$ *tale che* $\mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n) = \mathbb{F}(\gamma)$.

Dimostrazione. Come prima dividiamo la dimostrazione in due casi.

1. Se $\mathbb{F}$ è finito allora poiché i δ_i sono tutti algebrici su $\mathbb{F}$ l'estensione $\mathbb{F} \subseteq \mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$ è finita, quindi anche $\mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$ è finito, analogamente al teorema precedente esiste $\gamma \in \mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$ tale che $\mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n) = \mathbb{F}(\gamma)$. Inoltre, essendo $\mathbb{F}(\gamma)$ campo di spezzamento del polinomio $x^{p^m} - x$ (dove $|\mathbb{F}(\gamma)| = p^m$) che ha tutte le radici distinte esso coinciderà con il polinomio minimo di γ su $\mathbb{F}$, da cui γ è separabile su $\mathbb{F}$.

2. Supponiamo $\mathbb{F}$ infinito. La dimostrazione è del tutto analoga al teorema precedente eccetto la separabilità di γ su $\mathbb{F}$ nel caso $n = 2$. Utilizzando la stessa notazione di prima abbiamo $\mathbb{F} \subseteq \mathbb{F}(\alpha, \beta)$ con α, β separabili su $\mathbb{F}$, $p_\alpha(x)$ il polinomio minimo di α in $\mathbb{F}$ e $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ le sue radici (distinte per ipotesi) con $r = \deg p_\alpha$, $p_\beta(x)$ il polinomio minimo di β in $\mathbb{F}$ e $\beta = \beta_1, \beta_2, \ldots, \beta_s$ le sue radici (distinte per ipotesi) con $s = \deg p_\beta$. Poiché $\mathbb{F}$ è infinito esiste $\lambda \in \mathbb{F}$ tale che

$$\lambda \neq \frac{\alpha_h - \alpha_i}{\beta_j - \beta_k} \quad \begin{array}{l} i, h \in \{1, \ldots, r\} \\ j, k \in \{1, \ldots, s\}, \quad j \neq k \end{array}.$$

   Per costruzione abbiamo $\alpha_i + \lambda\beta_j \neq \alpha_h + \lambda\beta_k$ al variare degli indici i, j, k, h. Sia $\gamma = \alpha + \lambda\beta$. Usando lo stesso procedimento della precedente dimostrazione abbiamo $\mathbb{F}(\gamma) = \mathbb{F}(\alpha, \beta)$. Proviamo che γ è separabile su $\mathbb{F}$. Sia $p_\gamma(x)$ il polinomio minimo di γ su $\mathbb{F}$ e sia

$$s(x) = \prod_{j=1}^{s} p_\alpha(x - \lambda\beta_i).$$

   Osserviamo che $s(\gamma) = s(\alpha + \lambda\beta) = 0$ in quanto per $j = 1$ risulta

$$p_\alpha(\gamma - \lambda\beta) = p_\alpha(\alpha + \lambda\beta - \lambda\beta) = p_\alpha(\alpha) = 0.$$

   Proviamo che $s(x) \in \mathbb{F}[x]$. Sia

$$S(x_1, x_2, \ldots, x_s, x) = \prod_{j=1}^{s} p_\alpha(x - \lambda x_j) \in \mathbb{F}[x_1, \ldots, x_s, x],$$

   esso è un polinomio simmetrico nelle $x_1, \ldots, x_s$, sviluppando i prodotti possiamo scrivere

$$S(x_1, \ldots, x_s, x) = \sum_{i=1}^{r \cdot s} q_i(x_1, \ldots, x_s) x^i$$

con $r \cdot s = \deg S$ e $q_i \in \mathbb{F}[x_1, \ldots, x_s]$ polinomi simmetrici per ogni $i \in \{1, \ldots, r \cdot s\}$. Per un precedente corollario sui polinomi simmetrici abbiamo che $q_i(\beta_1, \ldots, \beta_s) \in \mathbb{F}$, da cui

$$s(x) = S(\beta_1, \ldots, \beta_s, x) = \sum_{i=1}^{r \cdot s} q_i(\beta_1, \ldots, \beta_s) x^i \in \mathbb{F}[x].$$

Inoltre $s(\gamma) = 0 \Rightarrow p_\gamma(x) \mid s(x)$ in $\mathbb{F}[x]$. Osserviamo che $s(x)$ ha tutte le radici distinte, infatti

$$p_\alpha(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_r) \Rightarrow$$
$$\Rightarrow p_\alpha(x - \lambda\beta_j) = (x - \alpha_1 - \lambda\beta_j) \ldots (x - \alpha_r - \lambda\beta_j) =$$
$$= (x - (\alpha_1 + \lambda\beta_j)) \ldots (x - (\alpha_r + \lambda\beta_j))$$

da cui possiamo scrivere

$$s(x) = \prod_{j=1}^{s} p_\alpha(x - \lambda\beta_j) = \prod_{i=1}^{r} \prod_{j=1}^{s} (x - (\alpha_i + \lambda\beta_j))$$

quindi $s(x)$ ha tutte le radici distinte per la scelta di λ, ma dato che $p_\gamma(x) \mid s(x)$ ne segue che γ è separabile su $\mathbb{F}$. □

Vediamo adesso un esempio di estensione finita che non è né semplice né separabile.

Esempio 1.6.3. *Sia $\mathbb{K} = \mathbb{Z}_p(t, v)$ con t, v indeterminate su $\mathbb{Z}_p$. Poniamo $t^p = u, v^p = w$ (come dimostrato in un precedente esempio anche u e w sono indeterminate su $\mathbb{Z}_p$) e sia*

$$\mathbb{F} = \mathbb{Z}_p(u, w) \subseteq \mathbb{Z}_p(t, v) = \mathbb{K}.$$

Analogamente all'esempio precedente, t e v non sono separabili su $\mathbb{F}$ e hanno polinomi minimi su $\mathbb{F}$ rispettivamente $x^p - u, x^p - w \in \mathbb{F}[x]$. Quindi t ovviamente è algebrico su $\mathbb{F}$, inoltre v è algebrico su $\mathbb{F}(t)$ in quanto il polinomio $x^p - w$ visto in $\mathbb{F}(t)[x]$ continua a essere irriducibile per il criterio di Eisenstein. Dunque considerando la catena di estensioni $\mathbb{F} \subseteq \mathbb{F}(t) \subseteq \mathbb{F}(t, v) = \mathbb{K}$ ne segue $[\mathbb{K} : \mathbb{F}] = p^2$.
Per assurdo supponiamo che $\mathbb{F} \subseteq \mathbb{K}$ sia semplice, cioè $\exists z \in \mathbb{K} : \mathbb{F}(z) = \mathbb{K}$. Ma dato che $\mathbb{K} = \mathbb{Z}_p(t, v)$, z sarà del tipo

$$z = \frac{a_{0,0} + a_{1,0}t + a_{0,1}v + a_{1,1}tv + \ldots}{b_{0,0} + b_{1,0}t + b_{0,1}v + b_{1,1}tv + \ldots} \quad \text{con } a_{i,j}, b_{h,k} \in \mathbb{Z}_p$$

adesso dato che $ch(\mathbb{Z}_p) = p$, dal lemma (1.1.6) risulta

$$z^p = \frac{{a_{0,0}}^p + {a_{1,0}}^p t^p + {a_{0,1}}^p v^p + {a_{1,1}}^p t^p v^p + \ldots}{{b_{0,0}}^p + {b_{1,0}}^p t^p + {b_{0,1}}^p v^p + {b_{1,1}}^p t^p v^p + \ldots} = \frac{{a_{0,0}}^p + {a_{1,0}}^p u + {a_{0,1}}^p w + {a_{1,1}}^p uw + \ldots}{{b_{0,0}}^p + {b_{1,0}}^p u + {b_{0,1}}^p w + {b_{1,1}}^p uw + \ldots}$$

quindi $z^p \in \mathbb{Z}_p(u, w) = \mathbb{F}$, allora z è radice del polinomio $x^p - z^p \in \mathbb{F}[x]$, pertanto $[\mathbb{K} : \mathbb{F}] = p$, assurdo.
Osserviamo inoltre che per ogni $\lambda, \mu \in \mathbb{F}$ con $\lambda \neq \mu$, dal momento che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ non è semplice deve aversi

$$\mathbb{F} \subsetneq \mathbb{F}(t + \lambda v) \subsetneq \mathbb{K}$$

$$\mathbb{F} \subsetneq \mathbb{F}(t+\mu v) \subsetneq \mathbb{K}.$$

Proviamo che $\mathbb{F}(t+\lambda v) \neq \mathbb{F}(t+\mu v)$*, infatti se si avesse l'ugualianza allora*

$$t+\lambda v \in \mathbb{F}(t+\lambda v)$$

$$t+\mu v \in \mathbb{F}(t+\lambda v)$$

da cui $t+\lambda v-(t+\mu v)=(\lambda-\mu)v \in \mathbb{F}(t+\lambda v) \Rightarrow v \in \mathbb{F}(t+\lambda v)$ *dal momento che* $\lambda-\mu \neq 0$*, quindi anche* $t=(t+\lambda v)-\lambda v \in \mathbb{F}(t+\lambda v)$*, cioè* $\mathbb{F}(t+\lambda v)=\mathbb{F}(t,v)=\mathbb{K}$*, assurdo. Da ciò possiamo concludere che tra* $\mathbb{F}$ *e* $\mathbb{K}$ *ci sono infiniti campi intermedi, dato che* $|\mathbb{F}|=|\mathbb{Z}_p(u,v)|=\infty$*.*

1.7 Estensioni normali

Teorema 1.7.1. *Sia* $f \in \mathbb{F}[x]$*,* $\mathbb{K}$ *campo di spezzamento di* f *e* $g \in \mathbb{F}[x]$ *irriducibile. Se* g *ha una radice in* $\mathbb{K}$ *allora* g *ha tutte le radici in* $\mathbb{K}$*.*

Dimostrazione. Possiamo supporre che f e g siano monici, quindi essendo g irriducibile e monico esso è il polinomio minimo di ogni sua radice. Siano $\alpha_1,\alpha_2,\ldots,\alpha_n \in \mathbb{K}$ le radici di f, allora

$$\mathbb{K}=\mathbb{F}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\mathbb{F}[\alpha_1,\alpha_2,\ldots,\alpha_n],$$

quindi se $\beta \in \mathbb{K}$ è una radice di g allora $\beta=h(\alpha_1,\alpha_2,\ldots,\alpha_n)$, con $h(x_1,x_2,\ldots,x_n) \in \mathbb{F}[x_1,x_2,\ldots,x_n]$. Sia

$$s(x)=\prod_{\sigma\in S_n}\left(x-h(\alpha_{\sigma(1)},\alpha_{\sigma(2)},\ldots,\alpha_{\sigma(n)})\right) \in \mathbb{K}[x],$$

dato che $\beta=h(\alpha_1,\alpha_2,\ldots,\alpha_n)$ abbiamo $s(\beta)=0$. Proviamo che $s(x) \in \mathbb{F}[x]$. Sia

$$S(x_1,x_2,\ldots,x_n,x)=\prod_{\sigma\in S_n}\left(x-h(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})\right) \in \mathbb{F}[x_1,x_2,\ldots,x_n][x],$$

$S(x_1,x_2,\ldots,x_n,x)$ è simmetrico nelle $x_1,x_2,\ldots,x_n$, sviluppando i prodotti abbiamo

$$S(x_1,x_2,\ldots,x_n,x)=\sum_{i=0}^{n!} q_i(x_1,x_2,\ldots,x_n)x^i,$$

dal momento che $S(x_1,x_2,\ldots,x_n,x)=S(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)},x) \quad \forall\sigma\in S_n$, dal principio di identità dei polinomi applicato rispetto a x risulta che tutti i polinomi $q_i(x_1,x_2,\ldots,x_n)$ sono simmetrici. Per un precedente corollario, dato che $\alpha_1,\ldots,\alpha_n$ sono le radici di f, abbiamo $q_i(\alpha_1,\alpha_2,\ldots,\alpha_n) \in \mathbb{F}$ per ogni $i \in \{0,\ldots,n\}$, quindi otteniamo $S(\alpha_1,\ldots,\alpha_n,x)=s(x) \in \mathbb{F}[x]$. Inoltre essendo β radice di $s(x)$ allora $g(x)|s(x)$ in quanto g è il polinomio minimo di ogni sua radice. Ma per definizione $s(x)$ si fattorizza linearmente in $\mathbb{K}[x]$, ne segue che $g(x)$ ha tutte le radici in $\mathbb{K}$. □

Definizione 1.7.2. *Un'estensione* $\mathbb{F} \subseteq \mathbb{K}$ *algebrica è detta* ***normale*** *se ogni polinomio irriducibile di* $\mathbb{F}[x]$ *avente una radice in* $\mathbb{K}$ *ha tutte le radici in* $\mathbb{K}$*.*

Ad esempio l'estensione $\mathbb{F} \subseteq \overline{\mathbb{F}}$ è sempre normale.

Esempio 1.7.3. *L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ non è normale, infatti $x^3 - 2 \in \mathbb{Q}[x]$ è un polinomio irriducibile (per il criterio di Eisenstein) e ha solamente $\sqrt[3]{2}$ come radice in $\mathbb{Q}(\sqrt[3]{2})$. Pertanto dall'ultimo teorema segue che $\mathbb{Q}(\sqrt[3]{2})$ non può essere campo di spezzamento di alcun polinomio in $\mathbb{Q}[x]$.*

Proposizione 1.7.4. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. $\mathbb{K}$ è campo di spezzamento di un polinomio in $\mathbb{F}[x]$ se e solo se $\mathbb{F} \subseteq \mathbb{K}$ è finita e normale.*

Dimostrazione.

$\Rightarrow$ Segue dal teorema precedente.

$\Leftarrow$ Per ipotesi $\mathbb{F} \subseteq \mathbb{K}$ è finita, cioè è algebrica e finitamente generata, quindi esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ algebrici su $\mathbb{F}$ tali che $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Sia, per ogni $i = 1, \ldots, n$, $p_i(x)$ il polinomio minimo di α_i su $\mathbb{F}$ e sia $f(x) = p_1(x) \ldots p_n(x)$. Dato che $p_i(x)$ è irriducibile con radice $\alpha_i \in \mathbb{K}$, dal fatto che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è normale sappiamo che $p_i(x)$ si spezza linearmente in $\mathbb{K}[x]$, quindi anche $f(x)$ si spezza linearmente in $\mathbb{K}[x]$, cioè $\mathbb{K}$ è campo di spezzamento di $f(x)$.

□

Teoria di Galois

2.1 Isomorfismi di campi

Un omomorfismo di campi non è altro che un omomorfismo di anelli tra due campi. Come abbiamo visto in (1.1.2) ogni omomorfismo di campi non nullo è unitario, ed inoltre, poiché un campo è privo ideali non banali, è anche iniettivo.

Definizione 2.1.1. *Un omomorfismo di campi non nullo $\varphi : \mathbb{F} \to \mathbb{K}$ è detto* ***isomorfismo*** *di $\mathbb{F}$ in $\mathbb{K}$ o anche* ***immersione*** *di $\mathbb{F}$ in $\mathbb{K}$.*

L'uso del termine "isomorfismo" nella precedente definizione è improprio, infatti in questo caso abbiamo che $\mathbb{F}$ è isomorfo a $\varphi(\mathbb{F}) \subseteq \mathbb{K}$, quindi $\mathbb{F}$ e $\mathbb{K}$ risulteranno isomorfi se e solo se φ è anche suriettivo.

Proposizione 2.1.2. *Se $\varphi : \mathbb{F} \to \mathbb{K}$ è un isomorfismo di $\mathbb{F}$ in $\mathbb{K}$ allora $ch(\mathbb{F}) = ch(\mathbb{K})$. Inoltre se $P_{\mathbb{F}}$ e $P_{\mathbb{K}}$ sono i campi primi rispettivamente di $\mathbb{F}$ e di $\mathbb{K}$ allora $\varphi(P_{\mathbb{F}}) = P_{\mathbb{K}}$.*

Dimostrazione. Dalla definizione di caratteristica, poiché $\varphi(n{\cdot}1_{\mathbb{F}}) = n{\cdot}\varphi(1_{\mathbb{F}}) = n{\cdot}1_{\mathbb{K}}$ segue facilmente $ch(\mathbb{F}) = ch(\mathbb{K})$. Da (1.1.10) sappiamo che $P_{\mathbb{F}} \simeq P_{\mathbb{K}}$, inoltre dalla minimalità di $P_{\mathbb{K}}$ abbiamo $P_{\mathbb{K}} \subseteq \varphi(P_{\mathbb{F}}) \simeq P_{\mathbb{F}}$ da cui segue $P_{\mathbb{K}} = \varphi(P_{\mathbb{F}})$. □

Sia $\varphi : \mathbb{K} \to \mathbb{K}$ un automorfismo. Dal fatto che $\varphi(a \cdot 1) = a \cdot \varphi(1) = a \cdot 1$ segue che φ ristretto al campo primo P di $\mathbb{K}$ ci dà l'identità su P.

Definizione 2.1.3. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $\varphi : \mathbb{F} \to \mathbb{E}$ un isomorfismo di $\mathbb{F}$ in $\mathbb{E}$. Un'****estensione*** *di φ a $\mathbb{K}$ è un isomorfismo di campi $\sigma : \mathbb{K} \to \mathbb{E}$ tale che $\sigma_{|\mathbb{F}} = \varphi$.*

Proposizione 2.1.4. *Se $\varphi : \mathbb{F} \to \overline{\mathbb{F}}$ è l'immersione canonica (è un isomorfismo da $\mathbb{F}$ in $\overline{\mathbb{F}}$), $\alpha \in \overline{\mathbb{F}}$ e $\mathbb{K} = \mathbb{F}(\alpha)$ allora φ si estende a $\mathbb{K}$ in al più $n = [\mathbb{K} : \mathbb{F}] = \deg p_\alpha^{\mathbb{F}}(x)$ modi.*

Dimostrazione. Banalmente esiste almeno un'estensione di φ a $\mathbb{K}$, basta considerare l'immersione canonica di $\mathbb{K}$ in $\overline{\mathbb{F}}$. Sia $\phi : \mathbb{K} \to \overline{\mathbb{F}}$ un'estensione di φ a $\mathbb{K}$. Essendo α algebrico su $\mathbb{F}$ allora $\mathbb{K} = \mathbb{F}(\alpha) = \mathbb{F}[\alpha]$. Pertanto se $\beta \in \mathbb{K} = \mathbb{F}[\alpha]$ si ha

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \quad b_i \in \mathbb{F}$$

da cui

$$\phi(\beta) = b_0 + b_1\phi(\alpha) + \ldots + b_{n-1}\phi(\alpha)^{n-1},$$

in quanto $b_i \in \mathbb{F}$ e $\phi_{|\mathbb{F}} = \varphi$. Ne segue che l'estensione ϕ è univocamente determinata da $\phi(\alpha)$. Se

$$p_\alpha^{\mathbb{F}}(x) = a_0 + a_1x + \ldots + a_nx^n$$

è il polinomio minimo di α in $\mathbb{F}$, risulta

$$p_\alpha^{\mathbb{F}}(\phi(\alpha)) = a_0 + a_1\phi(\alpha) + \ldots + a_n\phi(\alpha)^n =$$

$$= \phi(a_0) + \phi(a_1)\phi(\alpha) + \ldots + \phi(a_n)\phi(\alpha^n) =$$

$$= \phi(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = \phi(0) = 0.$$

Dunque $\phi(\alpha) \in \overline{\mathbb{F}}$ deve essere una delle n radici di $p_\alpha^{\mathbb{F}}(x)$. Ma dato che $\phi(\alpha)$ determina univocamente segue che ci sono al più n estensioni di ϕ. □

Osservazione 2.1.5. *Se $\alpha \in \mathbb{K}$ è separabile su $\mathbb{F}$, allora φ si estende a $\mathbb{K} = \mathbb{F}(\alpha)$ in esattamente n modi. Infatti per ogni radice α_i di $p_\alpha^{\mathbb{F}}(x)$ possiamo considerare l'estensione $\phi : \mathbb{K} \to \overline{\mathbb{F}}$ con $\phi(\alpha) = \alpha_i$, essendo le radici di $p_\alpha^{\mathbb{F}}(x)$ tutte distinte avremo almeno n estensioni.*

Definizione 2.1.6. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione algebrica, definiamo*

$$\mathscr{I}(\mathbb{K}/\mathbb{F}) = \{\psi : \mathbb{K} \to \overline{\mathbb{F}} : \psi \text{ isomorfismo di } \mathbb{K} \text{ in } \overline{\mathbb{F}},\ \psi_{|\mathbb{F}} = 1_{\mathbb{F}}\}$$

Teorema 2.1.7. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione finita allora*

$$|\mathscr{I}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}].$$

Se ciascuno dei generatori dell'estensione $\mathbb{F} \subseteq \mathbb{K}$ è separabile su $\mathbb{F}$, allora vale l'uguaglianza.

Dimostrazione. Per ipotesi $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, $n = [\mathbb{K} : \mathbb{F}]$ con α_i algebrici su $\mathbb{F}$. Consideriamo la catena di estensioni

$$\mathbb{F} \subseteq \mathbb{F}(\alpha_1) \subseteq \mathbb{F}(\alpha_1, \alpha_2) \subseteq \ldots \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r)$$

e poniamo $m_i = [\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_i) : \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})]$, quindi $n = m_1 m_2 \ldots m_r$. Dalla proposizione precedente sappiamo che l'immersione canonica $\varphi : \mathbb{F} \to \overline{\mathbb{F}}$ si estende a $\mathbb{F}(\alpha_1)$ in al più m_1 modi, ognuna di queste estensioni si estende a sua volta a $\mathbb{F}(\alpha_1, \alpha_2)$ in al più m_2 modi, e così via fino a $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbb{K}$. Ne segue che

$$|\mathscr{I}(\mathbb{K}/\mathbb{F})| \leq m_1 m_2 \ldots m_r = n = [\mathbb{K} : \mathbb{F}].$$

Nel caso in cui ciascuno degli α_i è separabile su $\mathbb{F}$, dal teorema dell'elemento primitivo (versione forte) esiste $\gamma \in \mathbb{K}$ separabile su $\mathbb{F}$ tale che $\mathbb{K} = \mathbb{F}(\gamma)$. La tesi adesso segue facilmente dalla proposizione e dall'osservazione precedente. □

Osservazione 2.1.8. *Sia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ una catena di estensioni algebriche. Risulta*

$$\mathscr{I}(\mathbb{K}/\mathbb{L}) \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F}),$$

infatti, essendo $\mathbb{F} \subseteq \mathbb{L}$ algebrica si ha $\overline{\mathbb{F}} = \overline{\mathbb{L}}$, quindi ogni estensione dell'immersione $\psi : \mathbb{L} \to \overline{\mathbb{F}}$ può essere vista come estensione di $\psi_{|\mathbb{F}}$.

Definizione 2.1.9. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione algebrica e $T \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})$. Definiamo*

$$\mathbb{K}^T = \{\alpha \in \mathbb{K} : \phi(\alpha) = \alpha, \forall \phi \in T\}.$$

É di facile dimostrazione che $\mathbb{K}^T$ risulta un campo, esso è detto ***campo fissato da*** *T.*

Osservazione 2.1.10. *Dalla definizione per ogni $T \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})$ risulta $\mathbb{F} \subseteq \mathbb{K}^T \subseteq \mathbb{K}$. Inoltre abbiamo già visto che per ogni campo intermedio $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ abbiamo $\mathscr{I}(\mathbb{K}/\mathbb{L}) \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})$. Dunque, posti $\mathcal{A} = \{\mathbb{L} \text{ campo } : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\}, \mathcal{B} = \{T \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})\}$, ha senso considerare le due applicazioni*

$$\epsilon : \mathcal{A} \to \mathcal{B}, \quad \epsilon(\mathbb{L}) = \mathscr{I}(\mathbb{K}/\mathbb{L})$$

$$\eta : \mathcal{B} \to \mathcal{A}, \quad \eta(T) = \mathbb{K}^T.$$

Quindi se $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ allora $(\eta \circ \epsilon)(\mathbb{L}) = \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}$, mentre se $T \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})$ allora $(\epsilon \circ \eta)(T) = \mathscr{I}(\mathbb{K}/\mathbb{K}^T)$. Inoltre dalle definizioni si ha

$$\mathbb{L} \subseteq \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})} = (\eta \circ \epsilon)(\mathbb{L})$$

$$T \subseteq \mathscr{I}(\mathbb{K}/\mathbb{K}^T) = (\epsilon \circ \eta)(T).$$

Utilizzando la notazione dell'osservazione precedente, vogliamo studiare i casi in cui $\epsilon \circ \eta = 1_{\mathcal{A}}$ e $\eta \circ \epsilon = 1_{\mathcal{B}}$.

Lemma 2.1.11. *Per ogni $\mathbb{L} \in \mathcal{A}$ si ha $\mathscr{I}(\mathbb{K}/\mathbb{L}) = \mathscr{I}(\mathbb{K}/\mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})})$.*

Dimostrazione.

- $\subseteq$ Sia $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{L})$, per definizione $\forall \alpha \in \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}$ risulta $\varphi(\alpha) = \alpha$. Dunque, sempre per definizione, si ha $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})})$.
- $\supseteq$ Segue dal fatto che $\mathbb{L} \subseteq \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}$

□

Proposizione 2.1.12. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione finita e separabile allora per ogni $\mathbb{L} \in \mathcal{A}$ si ha $\mathbb{L} = \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}$ (cioè $\eta \circ \epsilon = 1_{\mathcal{A}}$).*

Dimostrazione. Per ipotesi l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è finita e separabile, quindi lo è anche $\mathbb{E} \subseteq \mathbb{K}$ per ogni $\mathbb{E} \in \mathcal{A}$. In base al teorema precedente abbiamo

$$[\mathbb{K} : \mathbb{L}] = |\mathscr{I}(\mathbb{K}/\mathbb{L})| = |\mathscr{I}(\mathbb{K}/\mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})})| = [\mathbb{K} : \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}]$$

da cui essendo $\mathbb{L} \subseteq \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})} \subseteq \mathbb{K}$ ne segue $[\mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})} : \mathbb{L}] = 1$, cioè $\mathbb{L} = \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{L})}$. □

Osservazione 2.1.13. *Se $\mathbb{F} \subseteq \mathbb{K}$ è finita e separabile allora $\eta \circ \epsilon = 1_{\mathcal{A}}$. Pertanto ϵ è iniettiva, ciò vuol dire che $|\mathcal{A}| \leq |\mathcal{B}|$. Inoltre dal fatto che $|\mathscr{I}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$ ed essendo $\mathcal{B}$ l'insieme delle parti di $\mathscr{I}(\mathbb{K}/\mathbb{F})$, segue che la cardinalità di $\mathcal{B}$ è finita. Dunque anche $\mathcal{A}$ è insieme finito, o in altri termini esistono un numero finito di campi intermedi tra $\mathbb{F}$ e $\mathbb{K}$.*

2.2 Gruppo di Galois

Definizione 2.2.1. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi. Si chiama* ***gruppo di Galois*** *dell'estensione $\mathbb{F} \subseteq \mathbb{K}$ l'insieme*

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) = \{\varphi : \mathbb{K} \to \mathbb{K} : \varphi \text{ automorfismo }, \varphi_{|\mathbb{F}} = 1_{\mathbb{F}}\} \subseteq \mathrm{Aut}(\mathbb{K})$$

Proposizione 2.2.2. *$\mathcal{G}(\mathbb{K}/\mathbb{F})$ è un sottogruppo di* $\mathrm{Aut}(\mathbb{K})$.

Dimostrazione. Per ogni $\sigma_1, \sigma_2 \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ e ogni $\alpha \in \mathbb{F}$ abbiamo $(\sigma_1 \circ \sigma_2^{-1})(\alpha) = \sigma_1(\sigma_2^{-1}(\alpha)) = \sigma_1(\alpha) = \alpha$ ad cui $\sigma_1 \circ \sigma_2^{-1} \in \mathcal{G}(\mathbb{K}/\mathbb{F})$. □

Osservazione 2.2.3. *Se $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ è una catena di estensione di campi allora*

$$\mathcal{G}(\mathbb{K}/\mathbb{L}) \leq \mathcal{G}(\mathbb{K}/\mathbb{F}),$$

infatti ogni automorfismo di $\mathcal{G}(\mathbb{K}/\mathbb{L})$ lascia fisso $\mathbb{L}$, quindi lascia fisso anche $\mathbb{F} \subseteq \mathbb{L}$.

Osservazione 2.2.4. *Se $\mathbb{F} \subseteq \mathbb{K}$ è algebrica allora*

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F}).$$

Infatti in questo caso $\mathbb{F} \subseteq \mathbb{K} \subseteq \overline{\mathbb{F}}$ quindi per ogni $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ abbiamo $\varphi : \mathbb{K} \to \mathbb{K} \subseteq \overline{\mathbb{F}}$ con $\varphi_{|\mathbb{F}} = 1_{\mathbb{F}}$, cioè $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{F})$.
Inoltre se $\mathbb{F} \subseteq \mathbb{K}$ è anche finita allora

$$|\mathcal{G}(\mathbb{K}/\mathbb{F})| \leq |\mathscr{I}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}].$$

Osservazione 2.2.5. *Siano $\mathbb{F} \subseteq \mathbb{K}$ un'estensione algebrica, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ e $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{K}$. Se $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{F})$ allora $\varphi(f(\beta_1, \beta_2, \ldots, \beta_n)) = f(\varphi(\beta_1), \varphi(\beta_2), \ldots, \varphi(\beta_n))$ in quanto φ lascia fissi gli elementi di $\mathbb{F}$. In particolare se $\mathbb{F} \subseteq \mathbb{K}$ è anche finitamente generata allora esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ tali che $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$, quindi ogni $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{F})$ è univocamente determinato da $\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n)$. Inoltre*

$$p^{\mathbb{F}}_{\alpha_i}(\varphi(\alpha_i)) = \varphi(p^{\mathbb{F}}_{\alpha_i}(\alpha_i)) = \varphi(0) = 0$$

quindi $\varphi(\alpha_i)$ deve essere una radice di $p^{\mathbb{F}}_{\alpha_i}(x)$. Se vogliamo che $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F}) \subseteq \mathscr{I}(\mathbb{K}/\mathbb{F})$, allora $\varphi(\alpha_i)$ deve essere una radice di $p^{\mathbb{F}}_{\alpha_i}(x)$ che sta in $\mathbb{K}$.

Dall'osservazione precedente, se l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è anche normale, segue che ogni radice di $p^{\mathbb{F}}_{\alpha_i}$ sta automaticamente in $\mathbb{K}$ per cui abbiamo il seguente

Corollario 2.2.6. *Se l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è finita e normale allora*

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathscr{I}(\mathbb{K}/\mathbb{F})$$

Esempio 2.2.7. *L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ è finita ma non è normale, infatti il polinomio $x^3 - 2 \in \mathbb{Q}[x]$ è irriducibile in $\mathbb{Q}[x]$ ma ha una sola radice in $\mathbb{Q}(\sqrt[3]{2})$. Il gruppo di Galois $\mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ è formato solo dall'identità, mentre $\mathscr{I}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ha tre e elementi, precisamente gli isomorfismi di $\mathbb{Q}(\sqrt[3]{2})$ in $\overline{\mathbb{Q}}$ che mandano $\sqrt[3]{2}$ rispettivamente nelle tre radici del polinomio $x^3 - 2$. Pertanto in questo caso $\mathcal{G}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \subsetneq \mathscr{I}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.*

Analogamente a quanto fatto prima diamo la seguente definizione.

Definizione 2.2.8. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e $T \subseteq \mathcal{G}(\mathbb{K}/\mathbb{F})$. Definiamo*

$$\mathbb{K}^T = \{\alpha \in \mathbb{K} : \phi(\alpha) = \alpha, \forall \phi \in T\}.$$

É di facile dimostrazione che $\mathbb{K}^T$ risulta un campo, esso è detto ***campo fissato da*** *T.*

Lemma 2.2.9. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione di campi allora*

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathcal{G}(\mathbb{K}/\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})})$$

Dimostrazione. Del tutto analoga a quanto fatto in (2.1.11). □

Teorema 2.2.10. (Teorema di Galois) *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione finita. Sono equivalenti:*

1. *$\mathbb{F} \subseteq \mathbb{K}$ è normale e separabile.*
2. *$\mathbb{K}$ è campo di spezzamento di un polinomio $f \in \mathbb{F}[x]$ separabile.*
3. *$|\mathcal{G}(\mathbb{K}/\mathbb{L})| = [\mathbb{K} : \mathbb{L}]$ per ogni campo $\mathbb{L}$ tale che $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$.*
4. *$\mathbb{F} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}$.*

Dimostrazione.

(1) ⇒ (2) Per ipotesi esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ tali che $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Siano $p_i(x) = p^{\mathbb{F}}_{\alpha_i}(x)$. Consideriamo solo i polinomi $p_i(x)$ distinti e, a meno di riordinamento degli indici, supponiamo siano $p_1(x), p_2(x), \ldots, p_r(x)$. Sia $f(x) = p_1(x)p_2(x)\ldots p_r(x)$. Dato che ogni polinomio $p_i(x)$ è irriducibile in $\mathbb{F}[x]$ e ha una radice in $\mathbb{K}$, essendo l'estensione $\mathbb{F} \subseteq \mathbb{K}$ normale segue che tutte le radici di $p_i(x)$ stanno in $\mathbb{K}$, quindi $\mathbb{K}$ è campo di spezzamento di $f(x)$. Proviamo che f è separabile. Dato che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è separabile ogni $\alpha_i \in \mathbb{K}$ è separabile su $\mathbb{F}$ quindi ogni polinomio $p_i(x)$ ha tutte le radici distinte. Inoltre se per assurdo esiste $\beta \in \mathbb{K}$ tale che $p_i(\beta) = p_j(\beta) = 0$ allora $p_i(x) = p^{\mathbb{F}}_{\beta}(x) = p_j(x)$ in quanto $p_i(x)$ e $p_j(x)$ sono irriducibili e monici, contro il fatto che p_i e p_j sono distinti, assurdo. Ciò prova che f è separabile.

(2) ⇒ (3) Per ipotesi $\mathbb{K}$ è campo di spezzamento di $f \in \mathbb{F}[x]$, quindi l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è finita e normale, pertanto $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathscr{I}(\mathbb{K}/\mathbb{F})$. Inoltre $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con α_i radici distinte di f. Siano $p_i(x) = p^{\mathbb{F}}_{\alpha_i}(x)$, allora per ogni $i \in \{1, 2, \ldots, n\}$ $p_i(x)|f(x)$ da cui $p_i(x)$ è separabile, quindi ogni α_i è separabile su $\mathbb{F}$. Per (2.1.7) abbiamo

$$[\mathbb{K} : \mathbb{F}] = |\mathscr{I}(\mathbb{K}/\mathbb{F})| = |\mathcal{G}(\mathbb{K}/\mathbb{F})|.$$

Se adesso consideriamo un generico campo $\mathbb{L}$ tale che $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$, la tesi segue ripetendo quanto fatto in precedenza considerando il polinomio f in $\mathbb{L}[x] \supseteq \mathbb{F}[x]$.

(3) ⇒ (4) Dato che $\mathbb{F} \subseteq \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} \subseteq \mathbb{K}$, dal lemma precedente abbiamo $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathcal{G}(\mathbb{K}/\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})})$, quindi risulta

$$[\mathbb{K} : \mathbb{F}] = |\mathcal{G}(\mathbb{K}/\mathbb{F})| = |\mathcal{G}(\mathbb{K}/\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})})| = [\mathbb{K} : \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}],$$

da cui segue $\mathbb{F} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}$.

(4) $\Rightarrow$ (1) Dato che $\mathbb{F} \subseteq \mathbb{K}$ è finita, sappiamo che $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è finito, quindi poniamo $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$, con $\varphi_1 = 1_{\mathbb{K}}$. Sia $\alpha \in \mathbb{K}$ e siano $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ le immagini distinte di α tramite gli elementi $\varphi_i \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ in modo che $\alpha_i = \varphi_i(\alpha)$, quindi $m \leq n$. Osserviamo che $\varphi_i \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ induce una permutazione su $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subseteq \mathbb{K}$. Infatti $\varphi_i(\alpha_j) = \varphi_i(\varphi_j(\alpha)) = (\varphi_i \circ \varphi_j)(\alpha) = \varphi_k(\alpha) = \alpha_k$, quindi $\varphi_i(A) \subseteq A$, inoltre essendo φ_i un automorfismo di $\mathbb{K}$ essa è iniettiva e dato che A è un insieme finito allora φ_i è biettiva su A. Sia

$$h(x) = \prod_{i=1}^{m}(x - \alpha_i) = \sum_{i=0}^{m} a_i x^{n-i},$$

dove $a_i = (-1)^i \sigma_i(\alpha_1, \ldots, \alpha_m)$ con $\sigma_i(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ polinomi simmetrici elementari. Per quanto osservato prima abbiamo che per ogni $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ e ogni $i \in \{0, 1, \ldots, m\}$

$$\begin{aligned}\varphi(a_i) &= (-1)^i \varphi(\sigma_i(\alpha_1, \ldots, \alpha_m)) = (-1)^i \sigma_i(\varphi(\alpha_1), \ldots, \varphi(\alpha_m)) \\ &= (-1)^i \sigma_i(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(m)}) = (-1)^i \sigma_i(\alpha_1, \ldots, \alpha_m) = a_i\end{aligned}$$

per qualche $\tau \in S_m$. Dunque $a_i \in \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$ (per ipotesi), quindi $h(x) \in \mathbb{F}[x]$. Adesso poiché $h(\alpha) = 0$ allora $p_\alpha^{\mathbb{F}}(x) | h(x)$. Inoltre per ogni $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ abbiamo

$$p_\alpha^{\mathbb{F}}(\varphi(\alpha)) = \varphi(p_\alpha^{\mathbb{F}}(\alpha)) = \varphi(0) = 0$$

quindi ogni α_i è radice di $p_\alpha^{\mathbb{F}}(x)$, da cui $h(x) | p_\alpha^{\mathbb{F}}(x)$, cioè $h(x) = p_\alpha^{\mathbb{F}}(x)$. Per ipotesi gli α_i sono tutti distinti quindi α è separabile, inoltre abbiamo che ogni radice di $p_\alpha^{\mathbb{F}}(x)$ sta in $\mathbb{K}$. Ciò prova che l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è separabile e normale.

□

Osservazione 2.2.11. *Osserviamo che, se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione finita, dal lemma precedente segue che*

$$\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})})},$$

quindi, visto che $\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} \subseteq \mathbb{K}$ è un'estensione finita in quanto lo è $\mathbb{F} \subseteq \mathbb{K}$, per il punto (4) del teorema di Galois applicato al campo $\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}$ l'estensione $\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} \subseteq \mathbb{K}$ è di Galois.

Definizione 2.2.12. *Un'estensione $\mathbb{F} \subseteq \mathbb{K}$ si dice **di Galois** o **Galoissiana** se è finita, normale e separabile (o, equivalentemente, se è finita e soddisfa una delle quattro condizioni del teorema precedente).*

Corollario 2.2.13. *Sia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ una catena di estensioni di campi. Se $\mathbb{F} \subseteq \mathbb{K}$ è di Galois lo è anche $\mathbb{L} \subseteq \mathbb{K}$.*

Dimostrazione. Per ipotesi $\mathbb{K}$ è il campo di spezzamento di un polinomio $f(x) \in \mathbb{F}[x]$ separabile. Si ha $f(x) \in \mathbb{F}[x] \subseteq \mathbb{L}[x]$ da cui $\mathbb{K}$ è campo di spezzamento di $f(x) \in \mathbb{L}[x]$ separabile, pertanto $\mathbb{L} \subseteq \mathbb{K}$ è di Galois. □

Corollario 2.2.14. *Sia $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ un'estensione di campi. Se $\alpha_1, \alpha_2, \ldots, \alpha_n$ sono separabili su $\mathbb{F}$ allora $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è separabile.*

Dimostrazione. Dal teorema dell'elemento primitivo (versione forte) esiste $\gamma \in \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ tale che $\mathbb{F}(\gamma) = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con γ separabile su $\mathbb{F}$. Il polinomio $p_\gamma^{\mathbb{F}}(x)$ è separabile, sia $\mathbb{L}$ il suo campo di spezzamento. Dal teorema di Galois sappiamo che l'estensione $\mathbb{F} \subseteq \mathbb{L}$ è separabile da cui, visto che $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq \mathbb{L}$, allora anche $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è separabile. □

2.3 Corrispondenza di Galois

Osservazione 2.3.1. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di Galois. Dalla definizione, per ogni $T \subseteq \mathcal{G}(\mathbb{K}/\mathbb{F})$ risulta $\mathbb{F} \subseteq \mathbb{K}^T \subseteq \mathbb{K}$. Inoltre abbiamo già visto che per ogni campo intermedio $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ abbiamo $\mathcal{G}(\mathbb{K}/\mathbb{L}) \leq \mathcal{G}(\mathbb{K}/\mathbb{F})$. Dunque, posti $\mathcal{A} = \{\mathbb{L} \text{ campo } : \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}\}, \mathcal{B} = \{T \leq \mathcal{G}(\mathbb{K}/\mathbb{F})\}$, ha senso considerare le due applicazioni*

$$\epsilon : \mathcal{A} \to \mathcal{B}, \quad \epsilon(\mathbb{L}) = \mathcal{G}(\mathbb{K}/\mathbb{L})$$

$$\eta : \mathcal{B} \to \mathcal{A}, \quad \eta(T) = \mathbb{K}^T.$$

Dato che $\mathbb{F} \subseteq \mathbb{K}$ è di Galois, in base al teorema di Galois sappiamo che per ogni $\mathbb{L} \in \mathcal{A}$ si ha $\mathbb{L} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{K}^{\mathscr{I}(\mathbb{K}/\mathbb{F})}$, cioè $\eta \circ \epsilon = 1_{\mathcal{A}}$.

Il nostro obbiettivo sarà quello di provare che

- $H = \mathcal{G}(\mathbb{K}/\mathbb{K}^H) \quad \forall H \in \mathcal{B}$, cioè $\epsilon \circ \eta = 1_{\mathcal{B}}$.
- $\mathbb{F} \subseteq \mathbb{L}$ di Galois $\Leftrightarrow \mathcal{G}(\mathbb{K}/\mathbb{L}) \trianglelefteq \mathcal{G}(\mathbb{K}/\mathbb{F}) \quad \forall \mathbb{L} \in \mathcal{A}$.

Vediamo adesso una generalizzazione del punto (3) del teorema di Galois.

Proposizione 2.3.2. *Un'estensione finita $\mathbb{F} \subseteq \mathbb{K}$ è di Galois $\Leftrightarrow |\mathcal{G}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.*

Dimostrazione.

$\Rightarrow$ Segue dal punto (3) del teorema di Galois.

$\Leftarrow$ Risulta

$$[\mathbb{K} : \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}] \geq |\mathcal{G}(\mathbb{K}/\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})})| = |\mathcal{G}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}] \geq [\mathbb{K} : \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}],$$

dove l'ultima ugualianza è vera per ipotesi. Pertanto segue $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}]$ e poiché $\mathbb{F} \subseteq \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} \subseteq \mathbb{K}$ si ha $[\mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} : \mathbb{F}] = 1$, quindi $\mathbb{F} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}$. Dunque l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è di Galois.

□

Osservazione 2.3.3. *Sia $f \in \mathbb{F}[x]$ separabile con $n = \deg f(x)$ e sia $\mathbb{K}$ il suo campo di spezzamento. L'estensione $\mathbb{F} \subseteq \mathbb{K}$ è di Galois e inoltre se $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ sono le radici di f allora $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Osserviamo che ogni $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ induce una permutazione su $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, infatti, come abbiamo visto in precedenza, ogni $\varphi(\alpha_i)$ deve essere ancora una radice di f e φ è iniettiva (quindi biettiva) su $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. In altri termini, per ogni $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ esiste $\sigma \in S_n$ tale che $\varphi(\alpha_i) = \alpha_{\sigma(i)}$ per ogni $i \in \{1, 2, \ldots, n\}$. Consideriamo dunque l'applicazione $\psi : \mathcal{G}(\mathbb{K}/\mathbb{F}) \to S_n$ con $\psi(\varphi) = \sigma$ in modo tale che $\varphi(\alpha_i) = \alpha_{\sigma(i)}$. Facciamo vedere che ψ è un omomorfismo di gruppi. Siano $\varphi_1, \varphi_2 \in \mathcal{G}(\mathbb{K}/\mathbb{F})$, poniamo $\sigma_1 = \psi(\varphi_1)$, $\sigma_2 = \psi(\varphi_2)$, per ogni $i \in \{1, 2, \ldots, n\}$ si ha*

$$\alpha_{\psi(\varphi_1 \circ \varphi_2)(i)} = (\varphi_1 \circ \varphi_2)(\alpha_i) = \varphi_1(\varphi_2(\alpha_i)) = \varphi_1(\alpha_{\sigma_2(i)}) = \alpha_{\sigma_1(\sigma_2(i))} = \alpha_{(\sigma_1 \circ \sigma_2)(i)}$$

da cui

$$\psi(\varphi_1 \circ \varphi_2) = \sigma_1 \circ \sigma_2 = \psi(\varphi_1) \circ \psi(\varphi_2).$$

Inoltre ψ è iniettivo, infatti se $\varphi \in \ker \psi$ allora $\psi(\varphi)$ è l'identità su S_n, cioè per ogni $i \in \{1, 2, \ldots, n\}$ si ha $\varphi(\alpha_i) = \alpha_i$, quindi $\varphi = 1_{\mathbb{K}}$.
Abbiamo così dimostrato che $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è isomorfo a un sottogruppo di S_n[2]. Inoltre abbiamo che $[\mathbb{K} : \mathbb{F}] = |\mathcal{G}(\mathbb{K}/\mathbb{F})|$ divide $n!$ (in generale sappiamo che $[\mathbb{K} : \mathbb{F}] \leq n!$).

Definizione 2.3.4. *Un sottogruppo H di S_n è detto **transitivo** (o che **opera transitivamente** sull'insieme $\{1, 2, \ldots, n\}$) se $\forall i, j \in \{1, 2, \ldots, n\}$ esiste $\tau \in H$ tale che $\tau(i) = j$.*

Ad esempio S_n è transitivo, infatti basta considerare $\forall i, j \in \{1, 2, \ldots, n\}$ $\tau = (i\ j)$.

Proposizione 2.3.5. *Sia $f \in \mathbb{F}[x]$ separabile con $n = \deg f(x)$ e sia $\mathbb{K}$ il suo campo di spezzamento. Il sottogruppo $\psi(\mathcal{G}(\mathbb{K}/\mathbb{F})) \leq S_n$ è transitivo $\Leftrightarrow$ f è irriducibile*

Dimostrazione.

$\Rightarrow$ Sia $h(x) \in \mathbb{F}[x]$ un fattore irriducibile di $f(x)$ e sia $\alpha \in \mathbb{K}$ una sua radice. Per ipotesi, per ogni altra radice $\beta \in \mathbb{K}$ di $f(x)$ esiste $\varphi \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ tale che $\varphi(\alpha) = \beta$. Pertanto

$$h(\beta) = h(\varphi(\alpha)) = \varphi(h(\alpha)) = \varphi(0) = 0,$$

cioè ogni radice di f è anche radice di h, da cui $f(x) = h(x)$ irriducibile.

$\Leftarrow$ Senza perdita di generalità possiamo supporre $f(x)$ monico. Siano $\alpha, \beta \in \mathbb{K}$ due radici di f. Dato che f è irriducibile e monico abbiamo $p_\alpha^{\mathbb{F}}(x) = p_\beta^{\mathbb{F}}(x) = f(x)$, quindi

$$\mathbb{F}[\alpha] \simeq \frac{\mathbb{F}[x]}{(f(x))} \simeq \mathbb{F}[\beta]$$

dove i precedenti isomorfismi sono realizzati in questo modo:

$$p(\alpha) \to p(x) + (f(x)) \to p(\beta) \text{ con } p(x) \in \mathbb{F}[x]$$

quindi $\alpha \to x + (f(x)) \to \beta$ e per ogni $a \in \mathbb{F}$ risulta $a \to a + (f(x)) \to a$. Dunque esiste un isomorfismo $\phi : \mathbb{F}[\alpha] \to \mathbb{F}[\beta]$ tale che $\phi(\alpha) = \beta$ e $\phi_{|\mathbb{F}} = 1_{\mathbb{F}}$. A questo punto basta considerare un'estensione φ di ϕ a $\mathbb{K}$, avremo $\varphi \in \mathscr{I}(\mathbb{K}/\mathbb{F}) = \mathcal{G}(\mathbb{K}/\mathbb{F})$ (poiché $\mathbb{F} \subseteq \mathbb{K}$ è di Galois) con $\varphi(\alpha) = \beta$.

□

Proposizione 2.3.6. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione di Galois allora per ogni sottogruppo $H \leq \mathcal{G}(\mathbb{K}/\mathbb{F})$ risulta $H = \mathcal{G}(\mathbb{K}/\mathbb{K}^H)$.*

[2]Osserviamo che in generale $|\mathcal{G}(\mathbb{K}/\mathbb{F})|$ e n possono anche essere diversi, quindi quanto dimostrato è diverso dal teorema di Cayley

Dimostrazione. Dato che $\mathbb{F} \subseteq \mathbb{K}^H \subseteq \mathbb{K}$ dal teorema di Galois abbiamo $[\mathbb{K} : \mathbb{K}^H] = |\mathcal{G}(\mathbb{K}/\mathbb{K}^H)|$, quindi basta provare $[\mathbb{K} : \mathbb{K}^H] \leq |H|$, in questo modo si avrebbe

$$|\mathcal{G}(\mathbb{K}/\mathbb{K}^H)| = [\mathbb{K} : \mathbb{K}^H] \leq |H| \leq |\mathcal{G}(\mathbb{K}/\mathbb{K}^H)|$$

da cui $|H| = |\mathcal{G}(\mathbb{K}/\mathbb{K}^H)| \Rightarrow H = \mathcal{G}(\mathbb{K}/\mathbb{K}^H)$ in quanto insiemi finiti.
Essendo l'estensione $\mathbb{F} \subseteq \mathbb{K}$ di Galois allora anche $\mathbb{K}^H \subseteq \mathbb{K}$ è di Galois, in particolare essa è finita e separabile, pertanto dal teorema dell'elemento primitivo esiste $\alpha \in \mathbb{K}$ tale che $\mathbb{K}^H(\alpha) = \mathbb{K}$. Poniamo $H = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ e consideriamo il polinomio

$$h(x) = \prod_{i=1}^{n}(x - \varphi_i(\alpha)) = \sum_{i=0}^{n} a_i x^i$$

dove i coefficiente a_i sono i polinomi simmetrici elementari di n variabili calcolati in $\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_n(\alpha)$. Poiché in base al teorema di Cayley ogni $\varphi_i \in H$ induce una permutazione sull'insieme $\{\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_n(\alpha)\}$, infatti

$$\varphi_i\Big(\{\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_n(\alpha)\}\Big) = \Big\{(\varphi_i \circ \varphi_1)(\alpha), (\varphi_i \circ \varphi_2)(\alpha), \ldots, (\varphi_i \circ \varphi_n)(\alpha)\Big\},$$

allora $\varphi_j(a_i) = a_i \quad \forall i, j$, quindi $a_i \in \mathbb{K}^H$, cioè $h(x) \in \mathbb{K}^H[x]$. Inoltre α è una radice di $h(x)$ quindi $p_\alpha^{\mathbb{K}^H}(x) | h(x)$ da cui

$$[\mathbb{K} : \mathbb{K}^H] = \deg p_\alpha^{\mathbb{K}^H}(x) \leq \deg h(x) = |H|.$$

□

In base ai risultati precedenti e utilizzando la stessa notazione dell'osservazione (2.3.1) enunciamo il seguente

Teorema 2.3.7. (Teorema fondamentale della teoria di Galois)
Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di Galois. Valgono i seguenti fatti.

1. *Le applicazioni ϵ e η sono una l'inversa dell'altra.*
2. *$\forall \mathbb{L} \in \mathcal{A} \quad [\mathbb{K} : \mathbb{L}] = |\mathcal{G}(\mathbb{K}/\mathbb{L})|$.*
3. *Per ogni $\mathbb{L} \in \mathcal{A}$ l'estensione $\mathbb{F} \subseteq \mathbb{L}$ è di Galois $\Leftrightarrow \mathcal{G}(\mathbb{K}/\mathbb{L}) \trianglelefteq \mathcal{G}(\mathbb{K}/\mathbb{F})$ (in questo caso si ha $\mathcal{G}(\mathbb{L}/\mathbb{F}) \simeq \mathcal{G}(\mathbb{K}/\mathbb{F})/\mathcal{G}(\mathbb{K}/\mathbb{L})$).*

Dimostrazione. Proviamo il punto (3), i punti (1) e (2) seguono dai risultati precedenti.

$\Rightarrow$ Sia $\Omega : \mathcal{G}(\mathbb{K}/\mathbb{F}) \to \mathcal{G}(\mathbb{L}/\mathbb{F})$ con $\Omega(\sigma) = \sigma_{|\mathbb{L}}$. Ω è ben definita infatti per ogni $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F}) \quad \sigma(\mathbb{L}) \subseteq \overline{\mathbb{F}}$ quindi $\sigma_{|\mathbb{L}} \in \mathscr{I}(\mathbb{L}/\mathbb{F}) = \mathcal{G}(\mathbb{L}/\mathbb{F})$ in quanto l'estensione $\mathbb{F} \subseteq \mathbb{L}$ è di Galois. Mostriamo che Ω è un omomorfismo di gruppi. Siano $\sigma_1, \sigma_2 \in \mathcal{G}(\mathbb{K}/\mathbb{F})$, si ha

$$\Omega(\sigma_1 \circ \sigma_2) = (\sigma_1 \circ \sigma_2)_{|\mathbb{L}} = \sigma_{1|\mathbb{L}} \circ \sigma_{2|\mathbb{L}} = \Omega(\sigma_1) \circ \Omega(\sigma_2).$$

Dunque abbiamo

$$\ker \Omega = \{\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F}) : \Omega(\sigma) = \sigma_{|\mathbb{L}} = 1_{\mathbb{L}}\} = \mathcal{G}(\mathbb{K}/\mathbb{L}) \trianglelefteq \mathcal{G}(\mathbb{K}/\mathbb{F}),$$

da cui

$$\frac{\mathcal{G}(\mathbb{K}/\mathbb{F})}{\mathcal{G}(\mathbb{K}/\mathbb{L})} \simeq \operatorname{Im}\Omega \leq \mathcal{G}(\mathbb{L}/\mathbb{F}),$$

adesso

$$|\mathcal{G}(\mathbb{L}/\mathbb{F})| = [\mathbb{L}:\mathbb{F}] = \frac{[\mathbb{K}:\mathbb{F}]}{[\mathbb{K}:\mathbb{L}]} = \frac{|\mathcal{G}(\mathbb{K}/\mathbb{F})|}{|\mathcal{G}(\mathbb{K}/\mathbb{L})|} = |\operatorname{Im}\Omega| \leq |\mathcal{G}(\mathbb{L}/\mathbb{F})|$$

pertanto $|\mathcal{G}(\mathbb{L}/\mathbb{F})| = |\operatorname{Im}\Omega| \Rightarrow \mathcal{G}(\mathbb{L}/\mathbb{F}) = \operatorname{Im}\Omega$, da cui la tesi.

$\Leftarrow$ Proviamo che $\sigma(\mathbb{L}) \subseteq \mathbb{L}$ per ogni $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$. Per ipotesi $\mathcal{G}(\mathbb{K}/\mathbb{L}) \trianglelefteq \mathcal{G}(\mathbb{K}/\mathbb{F})$ pertanto se $\tau \in \mathcal{G}(\mathbb{K}/\mathbb{L})$ e $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ allora $\sigma^{-1}\tau\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{L})$ da cui, per ogni $\alpha \in \mathbb{L}$ risulta $(\sigma^{-1}\tau\sigma)(\alpha) = \alpha$, cioè $\tau(\sigma(\alpha)) = \sigma(\alpha)$. Dall'arbitrarietà di $\tau \in \mathcal{G}(\mathbb{K}/\mathbb{L})$ segue che $\sigma(\alpha) \in \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{L})} = \mathbb{L}$, poiché $\mathbb{L} \subseteq \mathbb{K}$ è di Galois. Dunque $\sigma(\mathbb{L}) \subseteq \mathbb{L}$. In altri termini, per ogni $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$, $\sigma_{|\mathbb{L}} \in \mathcal{G}(\mathbb{L}/\mathbb{F})$. In questo modo possiamo considerare come prima l'omomorfismo di gruppi $\Omega : \mathcal{G}(\mathbb{K}/\mathbb{F}) \to \mathcal{G}(\mathbb{L}/\mathbb{F})$ con $\Omega(\sigma) = \sigma_{|\mathbb{L}}$. Di nuovo

$$\ker\Omega = \{\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F}) : \Omega(\sigma) = \sigma_{|\mathbb{L}} = 1_{\mathbb{L}}\} = \mathcal{G}(\mathbb{K}/\mathbb{L}) \Rightarrow$$

$$\Rightarrow \frac{\mathcal{G}(\mathbb{K}/\mathbb{F})}{\mathcal{G}(\mathbb{K}/\mathbb{L})} \simeq \operatorname{Im}\Omega \leq \mathcal{G}(\mathbb{L}/\mathbb{F})$$

con ancora

$$|\mathcal{G}(\mathbb{L}/\mathbb{F})| \leq [\mathbb{L}:\mathbb{F}] = \frac{[\mathbb{K}:\mathbb{F}]}{[\mathbb{K}:\mathbb{L}]} = \frac{|\mathcal{G}(\mathbb{K}/\mathbb{F})|}{|\mathcal{G}(\mathbb{K}/\mathbb{L})|} = |\operatorname{Im}\Omega| \leq |\mathcal{G}(\mathbb{L}/\mathbb{F})|$$

di conseguenza $[\mathbb{L}:\mathbb{F}] = |\mathcal{G}(\mathbb{L}/\mathbb{F})|$ che, essendo $\mathbb{F} \subseteq \mathbb{L}$ finita, prova la tesi.

□

Definizione 2.3.8. *Sia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ una catena di estensioni di campi e $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$. Il campo $\sigma(\mathbb{L})$ è detto* ***coniugato*** *di $\mathbb{L}$.*

Proposizione 2.3.9. *Sia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ una catena di estensioni di campi. Per ogni $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ risulta*

$$\mathcal{G}(\mathbb{K}/\sigma(\mathbb{L})) = \sigma\mathcal{G}(\mathbb{K}/\mathbb{L})\sigma^{-1}.$$

Dimostrazione.

$$\tau \in \mathcal{G}(\mathbb{K}/\sigma(\mathbb{L})) \Leftrightarrow \forall\alpha \in \mathbb{L} \quad \tau(\sigma(\alpha)) = \sigma(\alpha) \Leftrightarrow \forall\alpha \in \mathbb{L} \quad (\sigma^{-1}\tau\sigma)(\alpha) = \alpha \Leftrightarrow$$

$$\Leftrightarrow \sigma^{-1}\tau\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{L}) \Leftrightarrow \tau \in \sigma\mathcal{G}(\mathbb{K}/\mathbb{L})\sigma^{-1}.$$

□

2.4 Teorema fondamentale dell'algebra

Teorema 2.4.1. (Teorema fondamentale dell'algebra) *Ogni polinomio in $\mathbb{C}[x]$ di grado positivo ammette radici in $\mathbb{C}$.*

Prima di dimostrare il teorema fondamentale dell'algebra (TFA), abbiamo bisogno di due lemmi.

Lemma 2.4.2. *Un polinomio $f(x) \in \mathbb{R}[x]$ monico di grado dispari ammette una radice in $\mathbb{R}$.*

Dimostrazione. Basta osservare che $\lim_{x\to\pm\infty} f(x) = \pm\infty$, quindi $\exists x_0, x_1 \in \mathbb{R}$ tali che $f(x_0) < 0$ e $f(x_1) > 0$, essendo $f(x)$ una funzione continua essa assume tutti i valori tra $f(x_0)$ e $f(x_1)$ (teorema dei valori intermedi), quindi esiste $\bar{x} \in [x_0, x_1]$ tale che $f(\bar{x}) = 0$. □

Lemma 2.4.3. *(TFA) $\iff$ ogni polinomio $f(x) \in \mathbb{R}[x]$ di grado positivo ha almeno una radice in $\mathbb{C}$.*

Dimostrazione.

- $\Rightarrow$ Ovvio
- $\Leftarrow$ Sia $f(x) \in \mathbb{C}[x]$ di grado positivo e $h(x) = f(x)\bar{f}(x)$. Risulta $\bar{h}(x) = \bar{f}(x)\bar{\bar{f}}(x) = \bar{f}(x)f(x) = h(x)$ quindi $h(x) \in \mathbb{R}[x]$. Per ipotesi $\exists\alpha \in \mathbb{C} : h(\alpha) = 0$, cioè $f(\alpha)\bar{f}(\alpha) = 0$. Adesso si ha $f(\alpha) = 0$ oppure $\bar{f}(\alpha) = 0$, cioè $0 = \bar{0} = \overline{\bar{f}(\alpha)} = f(\bar{\alpha})$, in ogni caso f ha una radice in $\mathbb{C}$.

□

In base al lemma precedente per dimostrare il TFA basta dimostrare che ogni polinomio a coefficienti in $\mathbb{R}$ ha $\mathbb{C}$ come campo di spezzamento.

Dimostrazione (TFA). Sia $f(x) \in \mathbb{R}[x]$ e $\mathbb{L}$ il campo di spezzamento di $f(x)(x^2+1) \in \mathbb{R}[x]$, quindi $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{L}$ e $\mathbb{L} = \mathbb{C}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbb{R}(i, \alpha_1, \alpha_2, \ldots, \alpha_r)$ dove le α_i sono le radici di f. L'estensione $\mathbb{R} \subseteq \mathbb{L}$ è di Galois in quanto è normale e finita essendo $\mathbb{L}$ campo di spezzamento di un polinomio in $\mathbb{R}[x]$, ed è separabile poiché $ch(\mathbb{R}) = 0$. Pertanto $|\mathcal{G}(\mathbb{L}/\mathbb{R})| = [\mathbb{L} : \mathbb{R}] = [\mathbb{L} : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2^{t+1}m$, con m dispari. Dal teorema di Sylow esiste $H \leq \mathcal{G}(\mathbb{L}/\mathbb{R}) : o(H) = 2^{t+1}$, quindi $\mathbb{R} \subseteq \mathbb{L}^H \subseteq \mathbb{L}$ con $[\mathbb{L} : \mathbb{L}^H] = |\mathcal{G}(\mathbb{L}/\mathbb{L}^H)| = |H| = 2^{t+1}$. Inoltre

$$[\mathbb{L}^H : \mathbb{R}] = \frac{[\mathbb{L} : \mathbb{R}]}{[\mathbb{L} : \mathbb{L}^H]} = \frac{2^{t+1}m}{2^{t+1}} = m.$$

Poiché l'estensione $\mathbb{R} \subseteq \mathbb{L}^H$ è finita e separabile per il teorema dell'elemento primitivo $\exists\beta \in \mathbb{L}^H : \mathbb{L}^H = \mathbb{R}(\beta)$. Il grado del polinomio $p_\beta^{\mathbb{R}}(x)$ è m che è dispari quindi dal lemma precedente deve risultare $m = 1$, altrimenti $p_\beta^{\mathbb{R}}(x)$ sarebbe riducibile. Dunque $\beta \in \mathbb{R} \Rightarrow \mathbb{L}^H = \mathbb{R}$ e risulta $[\mathbb{L} : \mathbb{R}] = 2^{t+1}$, quindi $[\mathbb{L} : \mathbb{C}] = 2^t$. Se per assurdo $t > 0$ allora esiste $N \trianglelefteq \mathcal{G}(\mathbb{L}/\mathbb{C}) : o(N) = 2^{t-1}$ da cui

$$[\mathbb{L} : \mathbb{L}^N] = |\mathcal{G}(\mathbb{L}/\mathbb{L}^N)| = |N| = 2^{t-1} \Rightarrow [\mathbb{L}^N : \mathbb{C}] = 2.$$

Pertanto deve esistere un polinomio $p(x) \in \mathbb{C}[x]$ irriducibile di grado 2. Verifichiamo che ciò è assurdo facendo vedere che, se $p(x) = ax^2 + bx + c$, allora esso ha per radici

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{C}.$$

Per fare ciò basta provare che la radice quadrata di un elemento in $\mathbb{C}$ sta in $\mathbb{C}$. Sia $z = \alpha + i\beta \in \mathbb{C}$, proviamo che esiste $w = x + iy \in \mathbb{C} : (x + iy)^2 = \alpha + i\beta$, si ha

$$\begin{cases} x^2 - y^2 = \alpha \\ 2xy = \beta \end{cases} \Rightarrow \begin{cases} x^2 + (-y^2) = \alpha \\ x^2(-y^2) = -\frac{\beta^2}{4} \end{cases}$$

troviamo x e y risolvendo l'equazione a coefficienti in $\mathbb{R}$ $t^2 - \alpha t - \frac{\beta^2}{4} = 0$, ottenendo

$$x^2 = \frac{\alpha + \sqrt{\alpha^2 + \beta^2}}{2}, \quad y^2 = \frac{-\alpha + \sqrt{\alpha^2 + \beta^2}}{2}$$

da cui scegliamo i valori di x e y per cui $2xy = \beta$. Ciò prova che ogni polinomio in $\mathbb{C}[x]$ di secondo grado è riducibile, assurdo. Quindi dev'essere $t = 0$ cioè $\mathbb{C} = \mathbb{L}$. □

2.5 Estensioni ciclotomiche

Definizione 2.5.1. *Una radice n-esima dell'unità $\epsilon \in \mathbb{C}$ è detta **primitiva** se è un generatore del gruppo moltiplicativo delle radici n-esime dell'unità.*

Osservazione 2.5.2. *Se $\epsilon \in \mathbb{C}$ è una radice n-esima primitiva dell'unità allora lo è anche ϵ^i se e solo se $MCD(n, i) = 1$. Dunque per ogni $n \in \mathbb{N}$ esistono $\varphi(n)$ radici n-esime primitive dell'unità, dove $\varphi : \mathbb{N} \to \mathbb{N}$ è la funzione di Eulero.*
Sappiamo che le radici n-esime dell'unità sono del tipo

$$\epsilon_k = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \in \mathbb{C}$$

quindi le radici n-esime primitive dell'unità sono tutte e sole le ϵ_i con $MCD(n, i) = 1$.

Definizione 2.5.3. *Se $\epsilon \in \mathbb{C}$ è una radice n-esima primitiva dell'unità l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)$ è detta **ciclotomica**.*

Osservazione 2.5.4. *Se $\epsilon \in \mathbb{C}$ è una radice n-esima primitiva dell'unità allora l'estensione ciclotomica $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon) = \mathbb{Q}(1, \epsilon, \epsilon^2, \ldots, \epsilon^{n-1})$ è di Galois, infatti è finita e normale in quanto $\mathbb{Q}(\epsilon)$ è campo di spezzamento di $x^n - 1 \in \mathbb{Q}[x]$ e separabile poiché $ch(\mathbb{Q}) = 0$.*

Vogliamo adesso calcolare il polinomio minimo di una radice n-esima primitiva dell'unità $\epsilon \in \mathbb{C}$ su $\mathbb{Q}$. Poniamo

$$f_n(x) = \prod_{MCD(n,i)=1} (x - \epsilon^i),$$

quindi $\deg f_n(x) = \varphi(n)$. Adesso per definizione sappiamo che

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \epsilon^i),$$

inoltre $MCD(n, i)$ è sempre un divisore di n, quindi al variare di d' divisore di n si ha

$$\prod_{i=0}^{n-1}(x - \epsilon^i) = \prod_{d'|n}\left(\prod_{MCD(n,i)=d'}(x - \epsilon^i)\right)$$

ma ad ogni divisore d' di n corrisponde un'altro divisore d di n tale che $dd' = n$, quindi $\epsilon^{d'}$ è una radice d-esima dell'unità. Adesso se $MCD(n, i) = d'$ allora $i = \lambda d'$ con

$$MCD(n, i) = MCD(dd', \lambda d') = d' \Rightarrow MCD(d, \lambda) = 1.$$

Dunque

$$\prod_{d'|n}\left(\prod_{MCD(n,i)=d'}(x - \epsilon^i)\right) = \prod_{d|n}\left(\prod_{MCD(d,\lambda)=1}\left(x - (\epsilon^{d'})^\lambda\right)\right) = \prod_{d|n} f_d(x).$$

Pertanto

$$x^n - 1 = \prod_{d|n} f_d(x).$$

Proposizione 2.5.5. *Per ogni $n \in \mathbb{N}$, $f_n(x) \in \mathbb{Z}[x]$.*

Dimostrazione. Procediamo per induzione su n. Se $n = 1$ banalmente $f_1(x) = x - 1 \in \mathbb{Z}[x]$.
Supponiamo che $f_m(x) \in \mathbb{Z}[x]$ per ogni $m < n$. Abbiamo

$$x^n - 1 = \prod_{d|n} f_d(x) = h(x)f_n(x) \quad \text{dove} \quad h(x) = \prod_{d|n, d<n} f_d(x) \in \mathbb{Z}[x],$$

quindi $f_n(x) = \frac{x^n-1}{h(x)} \in \mathbb{Z}(x) \subseteq \mathbb{Q}(x)$, ma essendo $f_n(x)$ un polinomio si ha $f_n(x) \in \mathbb{Q}[x]$. Infine esiste $a \in \mathbb{Z}$ tale che $af_n(x) \in \mathbb{Z}[x]$ è primitivo, scriviamo

$$a(x^n - 1) = h(x)(af_n(x))$$

da cui essendo $x^n - 1$ e $h(x)$ monici dal lemma di Gauss uguagliando i contenuti di ambo i membri otteniamo $a = 1$, cioè $f_n(x) \in \mathbb{Z}[x]$. □

Proposizione 2.5.6. *Per ogni $n \in \mathbb{N}$ e ogni radice n-esima primitiva dell'unità $\epsilon \in \mathbb{C}$ $f_n(x) = p_\epsilon^{\mathbb{Q}}(x)$.*

Dimostrazione. Poniamo per semplicità $p(x) = p_\epsilon^{\mathbb{Q}}(x)$. Dalla definizione $f_n(\epsilon) = 0$ quindi $p(x)|f_n(x)$, cioè esiste $h(x) \in \mathbb{Q}[x]$ tale che $f_n(x) = p(x)h(x)$. I polinomi $f_n(x)$ e $p(x)$ sono entrambi monici quindi anche $h(x)$ deve essere monico. Dunque $p(x), h(x) \in \mathbb{Q}[x]$ sono

primitivi, da cui esistono $a, b \in \mathbb{Z}$ tali che i polinomi $a\,p(x), b\,h(x) \in \mathbb{Z}[x]$ sono primitivi. Possiamo scrivere

$$ab\,f_n(x) = (a\,p(x))(b\,h(x)),$$

uguagliando i contenuti di ambo i membri in base al lemma di Gauss otteniamo $ab = 1$, cioè $a = b = \pm 1$ (visto che $a, b \in \mathbb{Z}$). In ogni caso $p(x), h(x) \in \mathbb{Z}[x]$.
Sia adesso $q \in \mathbb{N}$ primo con n ($MCD(n, q) = 1$), ci basta provare che $p(\epsilon^q) = 0$, infatti dall'arbitrarietà di q primo con n seguirebbe che ogni radice n-esima primitiva dell'unità è radice di $p(x)$ cioè $f_n(x)|p(x)$ da cui la tesi.
Supponiamo dapprima che q sia primo. Abbiamo

$$0 = f_n(\epsilon^q) = p(\epsilon^q)h(\epsilon^q).$$

Se $h(\epsilon^q) = 0$ allora ϵ è radice di $h(x^q)$, pertanto $p(x)|h(x^q)$, cioè $h(x^q) = p(x)l(x)$. Posto $h(x) = a_0 + a_1x + \ldots + a_rx^r$ allora, dato che $a^q \equiv a \pmod q$ (piccolo teorema di Fermat), considerando il polinomio $\bar{h}(x)$ come $h(x)$ visto in $\mathbb{Z}_q$, abbiamo (in base al Lemma 1.1.6)

$$\bar{h}(x^q) = a_0 + a_1x^q + \ldots + a_r(x^r)^q = a_0^q + a_1^qx^q + \ldots + a_n^q(x^r)^q =$$

$$= (a_0 + a_1x + \ldots + a_rx^r)^q = (\bar{h}(x))^q.$$

Dunque $\bar{p}(x)\bar{l}(x) = \bar{h}(x^q) = (\bar{h}(x))^q$, quindi ogni fattore irriducibile di $\bar{p}(x) \in \mathbb{Z}_q[x]$ è anche fattore di $(\bar{h}(x))^q$, cioè di $\bar{h}(x)$, ma

$$x^n - 1 = \bar{g}(x)\bar{f}_n(x) = \bar{g}(x)\bar{p}(x)\bar{h}(x),$$

quindi il polinomio $x^n - 1 \in \mathbb{Z}_q[x]$ ha radici multiple nel suo campo di spezzamento. Tuttavia $D(x^n - 1) = nx^{n-1}$ (con $n \neq 0 \pmod q$), pertanto $x^n - 1$ non può avere radici multiple, assurdo. Dunque $h(\epsilon^q) \neq 0$, cioè dev'essere $p(\epsilon^q) = 0$.
Sia adesso q primo con n non necessariamente primo e sia $q = q_1q_2 \ldots q_t$ la sua scomposizione in fattori primi, quindi

$$\epsilon^q = (((\epsilon^{q_1})^{q_2})^{\cdots})^{q_t},$$

per quanto dimostrato prima sappiamo che $p_\epsilon^{\mathbb{Q}}(\epsilon^{q_1}) = 0$ da cui $p_\epsilon^{\mathbb{Q}}(x) = p_{\epsilon^{q_1}}^{\mathbb{Q}}(x)$, analogamente $p_{\epsilon^{q_1}}^{\mathbb{Q}}((\epsilon^{q_1})^{q_2}) = 0$ da cui $p_{\epsilon^{q_1}}^{\mathbb{Q}}(x) = p_{(\epsilon^{q_1})^{q_2}}^{\mathbb{Q}}(x)$. Reiterando il processo fino a q_t otteniamo $p_\epsilon^{\mathbb{Q}}(x) = p_{\epsilon^q}^{\mathbb{Q}}(x)$, cioè $p(\epsilon^q) = 0$. □

Osservazione 2.5.7. *Dalla precedente proposizione segue che se $\epsilon \in \mathbb{C}$ è una radice n-esima primitiva dell'unità allora*

$$[\mathbb{Q}(\epsilon) : \mathbb{Q}] = \deg f_n(x) = \varphi(n).$$

Corollario 2.5.8. *Se $\epsilon \in \mathbb{C}$ è una radice n-esima primitiva dell'unità allora*

$$\mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \simeq U_n,$$

dove U_n è il gruppo moltiplicativo degli elementi di $\mathbb{Z}_n$ primi con n (cioè gli elementi invertibili di $\mathbb{Z}_n$).

Dimostrazione. Per quanto visto prima ogni elemento $\phi \in \mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ è univocamente determinato da $\phi(\epsilon)$ che deve essere una radice di $f_n(x)$, cioè una radice n-esima primitiva dell'unità, quindi $\phi(\epsilon) = \epsilon^i$ per qualche i primo con n, ovvero $i \in U_n$. Dunque

$$\mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q}) = \{\phi_i : \phi_i(\epsilon) = \epsilon^i, i \in U_n\}.$$

Sia allora $\psi : \mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \to U_n$ con $\psi(\phi_i) = i$. ψ è un isomorfismo in quanto è ovviamente suriettivo e iniettivo, inoltre è un'omomorfismo di gruppi, infatti

$$\psi(\phi_i \circ \phi_j) = \psi(\phi_{ij}) = ij = \psi(\phi_i)\psi(\phi_j).$$

□

2.6 Costruzioni con riga e compasso

In questo capitolo ci occuperemo di costruzioni che fanno uso solo di una riga (infinitamente lunga e non graduata), un compasso e due punti U e O che forniscono la lunghezza unitaria.

Definizione 2.6.1. *Una **costruzione con riga e compasso** (o **euclidea**) è una successione $A_1, A_2, \ldots, A_n$ di punti, rette o circonferenze dove $A_1 = O$, $A_2 = U$, soddisfacenti le proprietà*

1. *Se A_i è una retta allora deve essere una retta passante per due punti A_j, A_k con $j, k < i$.*

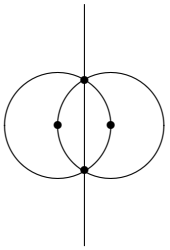
2. *Se A_i è una circonferenza allora ha centro in un punto A_j con $j < i$ e raggio di lunghezza uguale a quella di un segmento $\overline{A_s A_t}$ con $s, t < i$.*

3. *Se A_i è un punto allora è uguale a U o ad O oppure è intersezione di due rette o due circonferenze o una retta e una circonferenza già costruiti.*

Vediamo qualche esempio di costruzione con riga e compasso.

Esempio 2.6.2. *Costruiamo l'asse di un segmento dato:*

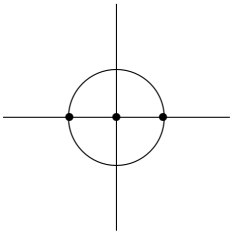
$A_1 = O$
$A_2 = U$
$A_3 =$ *circonferenza di centro O e raggio $\overline{OU}$*
$A_4 =$ *circonferenza di centro U e raggio $\overline{OU}$*
$A_5 =$ *primo punto di intersezione di A_3 e A_4*
$A_6 =$ *secondo punto di intersezione di A_3 e A_4*
$A_7 =$ *retta per A_5 e A_6*



A_7 è l'asse cercato.

Esempio 2.6.3. *Costruiamo un riferimento cartesiano:*

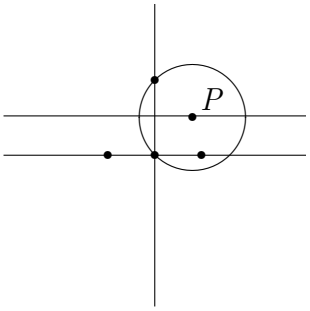
$A_1 = O$
$A_2 = U$
$A_3 =$ *retta per* O *e* U
$A_4 =$ *circonferenza di centro* O *e raggio* $\overline{OU}$
$A_5 =$ *punto di interesezione di* A_3 *e* A_4
$\vdots$
$A_{10} =$ *asse del segmento* $\overline{A_5U}$



Abbiamo omesso la costruzione di un asse di un segmento già vista nell'esempio precedente.

Esempio 2.6.4. *Costruiamo una retta parallela a una retta data passante per un punto esterno dato:*

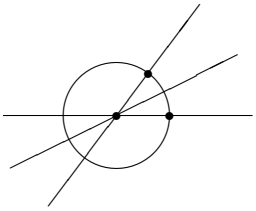
$A_1 = O$
$A_2 = U$
$A_3 =$ *retta per* O *e* U
$A_4 = P$ *(punto dato)*
$\vdots$
$A_9 =$ *asse del segmento* $\overline{OU}$
$A_{10} =$ *punto di intersezione di* A_9 *e* A_3
$A_{11} =$ *circonferenza di centro* P *e raggio* $\overline{A_{10}P}$
$A_{12} =$ *ulteriore punto d'intersezione tra* A_9 *e* A_{11}
$\vdots$
$A_{17} =$ *asse del segmento* $\overline{A_{10}A_{12}}$



A_{17} è la retta cercata. Abbiamo omesso la costruzione di un asse di un segmento già vista nell'esempio precedente. La precedente non è esattamente una costruzione euclidea, lo è nel caso in cui il punto P sia stato costruito precedentemente in qualche modo.

Esempio 2.6.5. *Costruiamo la bisettrice di un angolo:*

$A_1 = O$
$A_2 = U$
$A_3 =$ *retta per* O *e* U
$A_4 =$ *retta data*
$A_5 =$ *circonferenza di centro* O *e raggio* $\overline{OU}$
$A_6 =$ *punto di interesezione tra* A_4 *e* A_5
(vogliamo bisecare $U\hat{O}A_6$*)*
$\vdots$
$A_{11} =$ *asse del segmento* $\overline{UA_6}$



A_{11} è la bisettrice cercata. Abbiamo omesso la costruzione di un asse di un segmento già vista in un esempio precedente. Di nuovo la precedente non è esattamente una costruzione euclidea, lo è nel caso in cui la retta A_4 sia stata costruita precedentemente in qualche modo.

Definizione 2.6.6. *Un numero reale $a \in \mathbb{R}$ è detto* ***euclideo*** *(o* ***costruibile****) se è possibile costruire un segmento di lunghezza $|a|$ (o equivalentemente se è possibile costruire il punto $(a, 0)$). Un numero complesso $a + ib \in \mathbb{C}$ è detto* ***euclideo*** *(o* ***costruibile****) se sono euclidei $a, b \in \mathbb{R}$ (o equivalentemente se è possibile costruire il punto (a, b)).*

Osservazione 2.6.7. *Dalla definizione segue subito che se $a \in \mathbb{R}$ è costruibile allora lo è anche $-a$.*

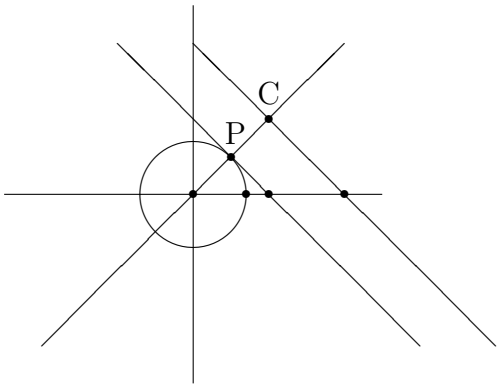
Proposizione 2.6.8. *Sia*

$$\mathbb{E} = \{a \in \mathbb{R} : a \text{ è euclideo}\}.$$

$\mathbb{E}$ è un campo e si ha $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{R}$.

Dimostrazione. Siano $a, b \in \mathbb{E}$, possiamo costruire i punti $P_1 = (a, 0)$ e $P_2 = (b, 0)$. Il segmento $\overline{P_1P_2}$ ha lunghezza $b - a \in \mathbb{E}$. Supponiamo adesso che $b > a > 0$, proviamo che $ab^{-1} \in \mathbb{E}$. Costruiamo un riferimento cartesiano e i punti $(b, 0), (b + a, 0)$. Costruiamo la bisettrice del primo e terzo quadrante e la circonferenza di centro O e raggio $\overline{OU}$, sia P il punto d'intersezione tra la circonferenza e la bisettrice. Costruiamo la retta r passante per i punti P e $(b, 0)$ e la retta s parallela a r e passante per il punto $(b + a, 0)$. Sia C il punto d'intersezione tra s e la bisettrice. Risulta

$$1 : b = \overline{PC} : a \Rightarrow \overline{PC} = ab^{-1} \in \mathbb{E}.$$



Nella costruzione abbiamo fatto uso delle costruzioni viste negli esempi precedenti.
É ovvio che $\mathbb{E} \subseteq \mathbb{R}$, da cui si ha $ch(\mathbb{E}) = 0$, dunque $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{R}$. □

Teorema 2.6.9. *Un numero reale $\alpha \in \mathbb{R}$ è euclideo se e solo se esiste una catena di campi*

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}_t \subseteq \mathbb{R}$$

tale che $\alpha \in \mathbb{K}_t$ e $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ per ogni $i \in \{0, 1, \ldots, t - 1\}$.

Dimostrazione.

⇒ Il punto $P = (\alpha, 0)$ è costruibile quindi esiste una successione di punti, rette e circonferenze

$$A_1, A_2, \ldots, A_r = P. \tag{2.2}$$

che sia una costruzione con riga e compasso. Sia l il numero di punti presenti in (2.2) (compreso P). Procediamo per induzione su l con l'ipotesi aggiuntiva che oltre

alle coordinate di P anche quelle degli altri punti appartengano a $\mathbb{K}_t$. Se $l = 1$ allora $O \equiv P$ quindi $\alpha = 0$ e la catena è $\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{R}$. Supponiamo adesso la tesi vera per quei punti che si possono costruire con una successione del tipo (2.2) in cui compaiono al massimo $l-1$ punti. Sia Q l'$(l-1)$-esimo punto della successione (2.2), per l'ipotesi induttiva esiste una catena di campi

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{n-1} \subseteq \mathbb{K}_n \subseteq \mathbb{R},$$

inoltre le coordinate dei punti di (2.2) appartengono a $\mathbb{K}_n$. Distinguiamo tre casi in cui il punto P è ottenuto tramite intersezione di due rette, di una retta e una circonferenza o di due circonferenze, dove le rette e le circonferenze hanno equazioni a coefficienti in $\mathbb{K}_n$.
Nel primo caso le coordinate di P sono ottenute da un sistema del tipo

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

sostituendo troviamo le soluzioni $x, y \in \mathbb{K}_n$ coordinate di P. La tesi è quindi ottenuta dalla catena $\mathbb{Q} = \mathbb{K}_0 \subseteq \ldots \subseteq \mathbb{K}_n \subseteq \mathbb{R}$.
Nel secondo caso le coordinate di P sono ottenute da un sistema del tipo

$$\begin{cases} a'x + b'y + c' = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}$$

eliminando una variabile otteniamo un'equazione del tipo $ax^2 + bx + c = 0$ con $a, b, c \in \mathbb{K}_n$, da cui

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{K}_n(\sqrt{b^2 - 4ac}).$$

Essendo $\sqrt{b^2 - 4ac}$ radice del polinomio $x^2 - b^2 + 4ac \in \mathbb{K}_n[x]$ il grado dell'estensione $\mathbb{K}_n \subseteq \mathbb{K}_n(\sqrt{b^2 - 4ac})$ può essere al più 2. Se $[\mathbb{K}_n(\sqrt{b^2 - 4ac}) : \mathbb{K}_n] = 1$ allora $x, y \in \mathbb{K}_n$ e analogamente al caso precedente la tesi è acquisita. Se invece $[\mathbb{K}_n(\sqrt{b^2 - 4ac}) : \mathbb{K}_n] = 2$ allora la tesi è ottenuta dalla catena di campi

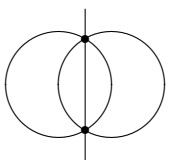
$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{n-1} \subseteq \mathbb{K}_n \subseteq \mathbb{K}_n(\sqrt{b^2 - 4ac}) = \mathbb{K}_{n+1} \subseteq \mathbb{R}.$$

Nel terzo caso le coordinate di P sono ottenute da un sistema del tipo

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

che si riduce facilmente a un sistema del tipo

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ (a' - a)x + (b' - b)y + (c' - c) = 0 \end{cases}$$



che rappresenta l'intersezione di una retta e una circonferenza, riconducendoci al caso precedente.

$\Leftarrow$ Procediamo per induzione su t. Se $t = 0$ allora $\alpha \in \mathbb{K}_0 = \mathbb{Q} \subseteq \mathbb{E}$ quindi α è euclideo. Supponiamo la tesi vera fino a $t-1$ e proviamo il teorema per t. Per ipotesi $\alpha \in \mathbb{K}_t$, adesso se $\alpha \in \mathbb{K}_{t-1}$ la tesi è acquisita, altrimenti se $\alpha \notin \mathbb{K}_{t-1}$ abbiamo

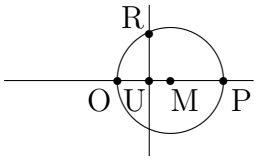
$$\mathbb{K}_{t-1} \subsetneq \mathbb{K}_{t-1}(\alpha) \subseteq \mathbb{K}_t \quad \text{con } [\mathbb{K}_t : \mathbb{K}_{t-1}] = 2,$$

allora dev'essere $[\mathbb{K}_{t-1}(\alpha) : \mathbb{K}_{t-1}] = 2$. Dunque $p_\alpha^{\mathbb{K}_{t-1}}(x) = x^2 + \beta x + \gamma \in \mathbb{K}_{t-1}[x]$ con $\beta, \gamma \in \mathbb{K}_{t-1}$ euclidei per l'ipotesi induttiva. Pertanto α, essendo radice di $p_\alpha^{\mathbb{K}_{t-1}}(x)$, è del tipo

$$\alpha = \frac{-\beta \pm \sqrt{\beta^2 - 4\gamma}}{2},$$

quindi α è costruibile se e solo se lo è $\sqrt{\beta^2 - 4\gamma} \in \mathbb{R}$. Dato che β e γ sono costruibili, è sufficiente dimostrare che in generale se $b \in \mathbb{R}^+$ è costruibile allora lo è anche $\sqrt{b}$ (si noti che $\beta^2 - 4\gamma \geq 0$ in quanto $\alpha \in \mathbb{R}$).
Supponiamo $b \in \mathbb{R}^+$ costruibile e di aver costruito il punto $P = (b + 1, 0)$, continuiamo la costruzione con i seguenti passaggi:

$A_1 = O$
$A_2 = U$
$\vdots$
$A_n = P$
$\vdots$
A_{n+5} = asse del segmento $\overline{OP}$
A_{n+6} = retta per O e U
A_{n+7} = punto d'intersezione tra A_{n+5} e $A_{n+6} = M$
A_{n+8} = circonferenza di centro M e raggio $\overline{OM}$
A_{n+9} = circonferenza di centro U e raggio $\overline{OU}$
A_{n+10} = punto d'intersezione tra A_{n+9} e A_{n+6}
$\vdots$
A_{n+15} = asse del segmento $\overline{OA_{n+10}}$
A_{n+16} = punto d'intersezione tra A_{n+8} e $A_{n+15} = R$



Il segmento cercato è $\overline{UR}$, infatti il triangolo ORP è rettangolo poiché è inscritto in una semicirconferenza quindi per il secondo teorema di Euclide l'altezza relativa all'ipotenusa $\overline{UR}$ è medio proporzionale tra le proiezioni dei due cateti sull'ipotenusa, cioè i segmenti $\overline{OU}$ e $\overline{UP}$ di lunghezza rispettivamente 1 e b. Pertanto si ha

$$1 : \overline{UR} = \overline{UR} : b \quad \Rightarrow \quad \overline{UR} = \sqrt{b}.$$

□

Corollario 2.6.10. *Se $\alpha \in \mathbb{R}$ è euclideo allora è anche algebrico e $\deg p_\alpha^{\mathbb{Q}}(x) = 2^m$ o in altri termini $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ per qualche $m \in \mathbb{N}$.*

Dimostrazione. Per ipotesi esiste una catena di campi

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}_t \subseteq \mathbb{R}$$

con $\alpha \in \mathbb{K}_t$ e $[\mathbb{K}_t : \mathbb{Q}] = 2^t$. Considerando la catena $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{K}_t$ abbiamo

$$2^t = [\mathbb{K}_t : \mathbb{Q}] = [\mathbb{K}_t : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m.$$

□

2.6.1 Tre problemi classici

Il precedente corollario ci permette di affrontare i famosi **tre problemi classici** dell'antichità:

1. **Quadratura del cerchio**, cioè il problema di costruire, mediante riga e compasso, un quadrato che abbia area uguale a un cerchio dato.
2. **Duplicazione del cubo**, cioè la costruzione, mediante riga e compasso, di un cubo di volume doppio a un cubo dato.
3. **Trisezione dell'angolo**, cioè la costruzione, mediante riga e compasso, di un angolo di ampiezza pari a un terzo di un angolo dato.

Il problema della quadratura del cerchio è equivalente alla costruzione di un segmento di lunghezza $\sqrt{\pi}$ che è equivalente alla costruibilità di π. Sappiamo però che π è trascendente (Lindemann, 1882) di conseguenza non essendo algebrico non può essere costruibile, ne segue l'impossibilità della quadratura del cerchio.

Il problema della duplicazione del cubo è equivalente alla costruzione di un segmento di lunghezza $\sqrt[3]{2}$. Sappiamo però che $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, quindi $\sqrt[3]{2}$ in base al corollario precedente non è costruibile, ne segue l'impossibilità di duplicare un cubo.

Il problema della trisezione di un dato angolo 3φ (che si suppone costruibile, nel senso che lo sia il punto $(\cos(3\varphi), \sin(3\varphi))$) è equivalente alla costruzione del punto $(\cos\varphi, \sin\varphi)$, cioè alla costruibilità di $\cos\varphi$ dato che $\sin\varphi$ è radice del polinomio $x^2 - 1 + \cos^2\varphi$. Poiché

$$\cos(3\varphi) = 4\cos^3\varphi - 3\cos\varphi,$$

allora $\cos\varphi$ è radice del polinomio $p(x) = 4x^3 - 3x - \cos(3\varphi) \in \mathbb{Q}(\cos(3\varphi))[x]$. Inoltre si ha $\cos(3\varphi) \in \mathbb{Q}(\cos(\varphi))$. Dunque

$$\mathbb{Q} \subseteq \mathbb{Q}(\cos(3\varphi)) \subseteq \mathbb{Q}(\cos(\varphi)).$$

Pertanto se $p(x)$ fosse irriducibile allora esso coninciderebbe con il polinomio minimo di $\cos(\varphi)$ su $\mathbb{Q}(\cos(3\varphi))$, quindi si avrebbe

$$[\mathbb{Q}(\cos(\varphi)) : \mathbb{Q}] = [\mathbb{Q}(\cos(\varphi)) : \mathbb{Q}(\cos(3\varphi))][\mathbb{Q}(\cos(3\varphi)) : \mathbb{Q}] = 3 \cdot [\mathbb{Q}(\cos(3\varphi)) : \mathbb{Q}] \neq 2^m,$$

da cui $\cos(\varphi)$ non sarebbe costruibile.
Viceversa se $p(x)$ fosse riducibile allora il polinomio minimo di $\cos\varphi$ su $\mathbb{Q}(\cos(3\varphi))$ sarà di grado al più 2. Sia

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}_t \subseteq \mathbb{R}$$

un catena di campi per cui $\cos(3\varphi) \in \mathbb{K}_t$ e $[\mathbb{K}_{i+1} : \mathbb{K}_t] = 2$ (una tale catena esiste poiché $\cos(3\varphi)$ è costruibile per ipotesi). Allora il polinomio minimo di $\cos(\varphi)$ su $\mathbb{K}_t$ divide il polinomio minimo di $\cos(\varphi)$ su $\mathbb{Q}(\cos(3\varphi))$ di grado al più due, quindi $\deg p^{\mathbb{K}_t}_{\cos(\varphi)}(x) \leq 2$, da cui possiamo allungare la catena con $\mathbb{K}_t \subseteq \mathbb{K}_t(\cos(\varphi))$ visto che quest'ultima è un'estensione di grado al più 2, da cui $\cos(\varphi)$ risulterà costruibile.
Dunque, per quanto detto finora, $\cos(\varphi)$ è costruibile se e solo se il polinomio $p(x)$ è riducibile.
Sia ad esempio $3\varphi = \frac{\pi}{3}$ allora $\cos(3\varphi) = \frac{1}{2}$ e $\cos\varphi$ è radice del polinomio $8x^2-6x-1 \in \mathbb{Q}[x]$ che è irriducibile non avendo radici razionali. Quindi $\cos\varphi$ non è costruibile.

2.6.2 Problema della ciclotomia

Il problema della ciclotomia o divisione della circonferenza (dal greco *ciclos* cerchio e *tomé* tagliare) è il problema di suddividere una circonferenza in n parti uguali o ciò che è lo stesso di inscrivere un poligono regolare di n lati in una circonferenza.

Costruire un poligono regolare di n lati $\mathcal{P}_n$ di centro O e con uno dei vertici coincidente con U è equivalente alla costruzione di tutti i suoi vertici $\mathcal{P}_{n,k}$ numerati rispetto a $k = 0, \ldots, n-1$ in senso antiorario i quali corrispondono alle radici n-esime dell'unità. Dato che queste ultime possono essere ottenute a partire dalla radice n-esima primitiva dell'unità

$$\epsilon = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

il problema si riduce alla costruibilità di $\epsilon \in \mathbb{C}$.

Teorema 2.6.11. *$\epsilon \in \mathbb{C}$ è euclideo $\iff$ $\varphi(n) = 2^m$ per qualche $m \in \mathbb{N}$.*

Dimostrazione.

$\Rightarrow$ Sia $\epsilon = a + ib$ con $a, b \in \mathbb{R}$ euclidei tali che $a^2 + b^2 = 1$. In particolare se a è euclideo allora esiste una catena di campi

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \ldots \subseteq \mathbb{K}_t \subseteq \mathbb{R}$$

con $a \in \mathbb{K}_t$ e $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ per ogni $i \in \{0, \ldots, t-1\}$. b è radice del polinomio $x^2 + a^2 - 1 \in \mathbb{K}_t[x]$ pertanto $[\mathbb{K}_t(b) : \mathbb{K}_t] \leq 2$, in ogni caso $[\mathbb{K}_t(b) : \mathbb{Q}] = 2^h$ dove h è uguale a t o $t+1$, ne segue $[\mathbb{K}_t(b,i) : \mathbb{Q}] = 2^{h+1}$ con $\epsilon \in \mathbb{K}_t(b,i)$. Adesso considerando la catena $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon) \subseteq \mathbb{K}_t(b,i)$, dato che $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)$ è un'estensione ciclotomica, abbiamo

$$2^{h+1} = [\mathbb{K}_t(b,i) : \mathbb{Q}] = [\mathbb{K}_t(b,i) : \mathbb{Q}(\epsilon)][\mathbb{Q}(\epsilon) : \mathbb{Q}] \Rightarrow \varphi(n) = [\mathbb{Q}(\epsilon) : \mathbb{Q}] = 2^m.$$

$\Leftarrow$ Basta provare che $a = \cos\left(\frac{2\pi}{n}\right)$ è costruibile. L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)$ è un'estensione ciclotomica, quindi è di Galois. Sia $\sigma : \mathbb{Q}(\epsilon) \to \overline{\mathbb{Q}}$ con $\sigma(\epsilon) = \overline{\epsilon}$. Osserviamo che $\sigma \in \mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ infatti σ manda ϵ in $\overline{\epsilon}$ che è ancora una radice di $p^{\mathbb{Q}}_{\epsilon}(x)$ e l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)$ è di Galois, quindi in particolare è normale. Abbiamo $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)} \subseteq \mathbb{Q}(\epsilon)$ dove

$$\mathcal{G}(\sigma) = \{1, \sigma\} \leq \mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q}), \quad [\mathbb{Q}(\epsilon) : \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}] = |\mathcal{G}(\sigma)| = 2.$$

Osserviamo che σ manda $\alpha \in \mathbb{Q}(\epsilon)$ nel suo coniugato $\overline{\alpha}$, quindi i numeri lasciati fissi da σ sono tutti e soli i numeri reali di $\mathbb{Q}(\epsilon)$, pertanto $\mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)} \subseteq \mathbb{R}$, in particolare $a = \cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}$. Essendo

$$\mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \simeq U_n \text{ abeliano con } |\mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q})| = [\mathbb{Q}(\epsilon) : \mathbb{Q}] = \varphi(n) = 2^m$$

abbiamo $\mathcal{G}(\sigma) \trianglelefteq \mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ quindi dal teorema fondamentale della teoria di Galois l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}$ è di Galois e inoltre

$$\mathcal{G}(\mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}/\mathbb{Q}) \simeq \frac{\mathcal{G}(\mathbb{Q}(\epsilon)/\mathbb{Q})}{\mathcal{G}(\sigma)} \Rightarrow |\mathcal{G}(\mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}/\mathbb{Q})| = 2^{m-1}.$$

Dalle proprietà dei gruppi di ordine la potenza di un primo esiste la catena di sottogruppi

$$\{e\} = H_0 \leq H_1 \leq \ldots \leq H_{m-2} \leq H_{m-1} = \mathcal{G}(\mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}/\mathbb{Q})$$

con $|H_i| = 2^i$ e $H_i \trianglelefteq H_{i+1}$ per ogni $i \in \{0, 1, \ldots, m-2\}$. Dunque per la corrispondenza di Galois esiste la catena di campi

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{m-2} \subseteq \mathbb{K}_{m-1} = \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)} \subseteq \mathbb{R}$$

con $\mathbb{K}_i = \left(\mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}\right)^{H_{m-1-i}}$, $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ per ogni $i \in \{0, 1, \ldots, m-2\}$ e $a = \cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}(\epsilon)^{\mathcal{G}(\sigma)}$ quindi a è costruibile. □

Ci chiediamo adesso per quali $n \in \mathbb{N}$ esiste $m \in \mathbb{N}$ tale che $\varphi(n) = 2^m$. Se

$$n = 2^r p_1^{s_1} \ldots p_h^{s_h}$$

è la scomposizione in fattori primi di n allora imponendo

$$\varphi(n) = 2^{r-1} p_1^{s_1-1}(p_1 - 1) \ldots p_h^{s_h-1}(p_h - 1) = 2^m$$

otteniamo $s_1 = 1, \ldots, s_h = 1$ e inoltre $p_i - 1$ deve essere una potenza di 2.

Proposizione 2.6.12. *Sia p primo dispari. Se $p - 1 = 2^k$ allora $k = 2^u$ per qualche $u \in \mathbb{N}$.*

Dimostrazione. Supponiamo che $k = 2^u m$ con m dispari, allora

$$p = \left(2^{2^u}\right)^m + 1 = (2^{2^u} + 1)\left((2^{2^u})^{m-1} - (2^{2^u})^{m-2} + \ldots + (-1)^{m-2} 2^{2^u} + (-1)^{m-1}\right)$$

ma essendo p primo deve risultare $m = 1$, cioè $p = 2^{2^u} + 1$. □

Definizione 2.6.13. *I primi della forma $2^{2^n} + 1$ sono detti **primi di Fermat**.*

Corollario 2.6.14. *Un poligono regolare di $n \geq 3$ lati è costruibile se e solo se*

$$n = 2^m \text{ oppure } n = 2^m p_1 p_2 \ldots p_s$$

dove $p_1, p_2, \ldots, p_s$ sono primi di Fermat distinti.

2.7 Gruppi Risolubili

Definizione 2.7.1. *Un gruppo G è detto **risolubile** se esiste una catena finita di sottogruppi di G*

$$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_{n-1} \leq K_n = G$$

*tale che $K_i \trianglelefteq K_{i+1}$ e K_{i+1}/K_i è abeliano per ogni $i \in \{0, 1, \ldots, n-1\}$. Una tale catena è detta **risolvente** per G.*

Osservazione 2.7.2. *Ogni gruppo G abeliano è risolubile tramite la catena risolvete $\{e\} \trianglelefteq G$.*
Ogni p-gruppo è risolubile tramite la catena

$$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_{n-1} \leq K_n = G$$

con $|K_i| = p^i$ e $K_i \trianglelefteq K_{i+1}$ con K_{i+1}/K_i abeliano in quanto $|K_{i+1}/K_i| = \frac{p^{i+1}}{p^i} = p$.

Lemma 2.7.3. *Siano G e G' due gruppi con G abeliano. Se esiste un omomorfismo $f : G \to G'$ suriettivo allora anche G' è abeliano.*

Dimostrazione. Per ipotesi per ogni $x', y' \in G'$ esistono $x, y \in G$ tali che $f(x) = x'$, $f(y) = y'$, da cui si ha

$$x'y' = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = y'x'. \qquad \square$$

Teorema 2.7.4. *Sia G un gruppo.*

1. *Se G è risolubile allora ogni sottogruppo $H \leq G$ è risolubile.*
2. *Se G è risolubile e $H \trianglelefteq G$ allora G/H è risolubile.*
3. *Se $N \trianglelefteq G$ e G/N sono risolubili allora G è risolubile.*
4. *Se G è finito e risolubile allora esiste una caten finita*

   $$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_{n-1} \leq K_n = G$$

   tale che K_{i+1}/K_i è ciclico di ordine primo.

Dimostrazione.

1. Per ipotesi esiste una catena risolvente per G

   $$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_{n-1} \leq K_n = G.$$

   Consideriamo la catena

   $$\{e\} = K_0 \cap H \leq K_1 \cap H \leq \ldots \leq K_{n-1} \cap H \leq K_n \cap H = G \cap H = H,$$

   abbiamo $K_i \cap H \trianglelefteq K_{i+1} \cap H$ infatti siano $k \in K_i \cap H$ e $h \in K_{i+1} \cap H$ allora $hkh^{-1} \in K_i \cap H$ in quanto $hkh^{-1} \in K_i$ essendo $K_i \trianglelefteq K_{i+1}$ e $hkh^{-1} \in H$ poiché $h, k \in H$.

Inoltre $(K_{i+1}\cap H)/(K_i\cap H)$ è abeliano infatti sia $\phi = \pi_{|K_{i+1}\cap H} : K_{i+1}\cap H \to K_{i+1}/K_i$ la restrizione a $K_{i+1}\cap H$ della proiezione canonica di K_{i+1} su K_{i+1}/K_i. Risulta

$$\ker\phi = \{k \in K_{i+1}\cap H : \phi(k) = K_i\} = \{k \in K_{i+1}\cap H : k \in K_i\} = K_i \cap H$$

pertanto dal teorema dell'isomorfismo

$$(K_{i+1}\cap H)/(K_i\cap H) \simeq \operatorname{Im}\phi \leq K_{i+1}/K_i \text{ abeliano},$$

ne segue che anche $(K_{i+1}\cap H)/(K_i\cap H)$ è abeliano, quindi H è risolubile.

2. Tramite la proiezione canonica π possiamo mettere in corrispondenza biunivoca i sottogruppi di G contenenti N e i sottogruppi di G/N. Per ipotesi esiste una catena risolvente per G
$$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_{n-1} \leq K_n = G.$$
Dal momento che $N \trianglelefteq G$ se $K \leq G$ è un sottogruppo di G allora lo è anche KN. Dunque possiamo considerare la catena

$$N = K_0N \leq K_1N \leq \ldots \leq K_nN = G.$$

Sia $H_i = \pi(K_iN) = K_iN/N \leq G/N$, proviamo che $H_i \trianglelefteq H_{i+1}$. Basta provare che $K_iN \trianglelefteq K_{i+1}N$, infatti da ciò seguirebbe $\pi(K_iN) \trianglelefteq \pi(K_{i+1}N)$, cioè $H_i \trianglelefteq H_{i+1}$. Sia $k_i\tilde{n} \in K_iN$ e $k_{i+1}n \in K_{i+1}N$, risulta

$$(k_{i+1}n)^{-1}(k_i\tilde{n})(k_{i+1}n) = n^{-1}k_{i+1}^{-1}k_i\tilde{n}k_{i+1}n$$

visto che $N \trianglelefteq G$ allora $k_{i+1}^{-1}\tilde{n}k_{i+1} = \tilde{n}' \in N$ quindi $\tilde{n}k_{i+1} = k_{i+1}\tilde{n}'$, da cui

$$n^{-1}k_{i+1}^{-1}k_i\tilde{n}k_{i+1}n = n^{-1}k_{i+1}^{-1}k_ik_{i+1}\tilde{n}'n.$$

Adesso visto che $K_i \trianglelefteq K_{i+1}$ allora $k_{i+1}^{-1}k_ik_{i+1} = k_i' \in K_i$. Con un ragionamento analogo al precedente otteniamo $n^{-1}k_i' = k_i''n' \in K_iN = NK_i$, pertanto

$$n^{-1}k_{i+1}^{-1}k_ik_{i+1}\tilde{n}'n = n^{-1}k_i'\tilde{n}'n = k_i''n'\tilde{n}'n \in K_iN$$

Proviamo che H_{i+1}/H_i è abeliano. In base al terzo teorema dell'isomorfismo abbiamo

$$H_{i+1}/H_i = \frac{NK_{i+1}/N}{NK_i/N} \simeq NK_{i+1}/NK_i$$

quindi ci basta provare che NK_{i+1}/NK_i è abeliano. Consideriamo l'immersione $\phi : K_{i+1} \to NK_{i+1}$ e la proiezione $\pi : NK_{i+1} \to NK_{i+1}/NK_i$ e sia $\psi = \pi\circ\phi$. Dunque si ha $\psi : K_{i+1} \to NK_{i+1}/NK_i$ con $\psi(k) = kNK_i = kK_iN$, quindi per qualunque $k' \in kK_i$ abbiamo $\psi(k') = k'K_iN = kK_iN$. Quest'ultima osservazione ci permette di concludere che $\ker\psi \supseteq K_i$ e che l'applicazione $\tilde{\psi} : K_{i+1}/K_i \to NK_{i+1}/NK_i$ con $\tilde{\psi}(kK_i) = \psi(k) = kNK_i$ è ben definita ed è un omomorfismo suriettivo. Pertanto dal lemma precedente segue che NK_{i+1}/NK_i è abeliano.

3. Per ipotesi esiste una catena risolvente per N

$$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_n = N,$$

e una catena risolvente per G/N

$$\{N\} = H_0 \leq H_1 \leq \ldots \leq H_m = G/N.$$

Sia $\pi : G \to G/N$ la proiezione naturale e $K_{n+i} = \pi^{-1}(H_i)$ per $i \in \{0, \ldots, m\}$. Abbiamo quindi $N \leq K_{n+i} \leq G$ con $K_{n+i} \trianglelefteq K_{i+1}$ visto che $H_i \trianglelefteq H_{i+1}$. Inoltre essendo $H_i = \pi(K_{n+i}) = K_{n+i}/N$ abbiamo

$$K_{n+i+1}/K_{n+i} \simeq \frac{K_{n+i+1}/N}{K_{n+i}/N} = H_{i+1}/H_i \text{ abeliano.}$$

Per quanto osservato prima la catena

$$\{e\} = K_0 \leq K_1 \leq \ldots \leq K_n \leq K_{n+1} \leq \ldots \leq K_{n+m} = G$$

è una catena risolvente per G.

4. Procedimao per induzione su $m = |G|$. Per $m = 1$ o $m = p$ primo la catena $\{e\} \leq G$ soddisfa le ipotesi. Supponiamo la tesi vera per gruppi di ordine minore di m e proviamolo per G, con $|G| = m$. Per ipotesi G ammette una catena risolvente

$$\{e\} \leq K_1 \leq \ldots \leq K_n = G.$$

Adesso $\overline{G} = G/K_{n-1}$ è abeliano, quindi $\overline{G}$ ammette un sottogruppo di ordine un qualunque divisore di $|\overline{G}|$. Sia p un divisore primo di $|\overline{G}|$ e $\overline{H} \leq \overline{G}$ con $|\overline{H}| = \frac{|\overline{G}|}{p}$. Consideriamo la proiezione naturale $\pi : G \to G/K_{n-1} = \overline{G}$. Sia $H = \pi^{-1}(\overline{H})$ con $|H| = \frac{|G|}{p}$, poiché $\overline{H} \trianglelefteq \overline{G}$ allora $H \trianglelefteq G$ con $|G/H| = p$, quindi G/H è ciclico. Dato che $|H| < |G|$ posso applicare l'ipotesi induttiva su H ottenendo la catena

$$\{e\} = H_0 \leq H_1 \leq \ldots \leq H_{k-1} \leq H_k = H \trianglelefteq G$$

da cui la tesi.

□

Osservazione 2.7.5. *Il punto 4 del precedente teorema ci dice che possiamo raffinare la catena risolvente di un gruppo risolubile finito in modo tale che K_{i+1}/K_i sia ciclico di ordine primo.*

A questo punto ci chiediamo per quali n il gruppo simmetrico S_n sia risolubile.

$n = 1$ $S_1 = \{e\}$ è banalmente risolubile.

$n = 2$ S_2 è abeliano quindi è risolubile.

$n = 3$ S_3 è risolubile. Considerando infatti $A_3 \trianglelefteq S_3$ il sottogruppo delle permutazioni pari la catena

$$\{e\} \leq A_3 \leq S_3$$

è una catena risolvente per S_3 in quanto $|S_3/A_3| = 2$ quindi S_3/A_3 è abeliano.

$n = 4$ S_4 è risolubile. Consideriamo infatti $A_4 \trianglelefteq S_4$ il gruppo delle permutazioni pari e

$$V = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq A_4$$

V è abeliano essendo $|V| = 4$. Inoltre osserviamo che due permutazioni coniugate hanno la stessa struttura ciclica in cicli disgiunti e viceversa, cioè due permutazioni con la stessa struttura sono coniugati in S_n. Da ciò otteniamo $V \trianglelefteq A_4$. Dunque la catena

$$\{e\} \leq V \leq A_4 \leq S_4$$

è risolvente per S_4.

Vediamo adesso di studiare la risolubilità di S_n per $n \geq 5$.

Lemma 2.7.6. *Per ogn $n \geq 5$, A_n è generato da 3-cicli.*

Dimostrazione. Sappiamo che ogni $\sigma \in A_n$ è prodotto di trasposizioni $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_{2k}$. Siano $i \neq j$, distinguiamo due casi:

1. $\tau_i = (a\,b), \tau_j = (a\,c) \Rightarrow \tau_i \circ \tau_j = (a\,c\,b)$.
2. $\tau_i = (a\,b), \tau_j = (c\,d) \Rightarrow \tau_i \circ \tau_j = (a\,c\,b)(c\,b\,d)$.

In ogni caso σ, dato che è una permutazione pari, risulterà prodotto di 3-cicli (non necessariamente disgiunti). □

Lemma 2.7.7. *Per ogni $n \geq 5$ due qualsiasi 3-cicli sono coniugati in A_n.*

Dimostrazione. Siano $\sigma_1 = (a\,b\,c), \sigma_2 = (e\,f\,g)$. Sappiamo che $\exists \tau \in S_n$ tale che

$$(a\,b\,c) = \tau(e\,f\,g)\tau^{-1} \text{ con } \tau = \begin{pmatrix} \ldots & a & b & c & \ldots \\ \ldots & e & f & g & \ldots \end{pmatrix}.$$

Se $\tau \in A_n$ la tesi è acquisita. Altrimenti, poiché $n \geq 5$ esistono $l, m \neq a, b, c$ tali che

$$\tau = \begin{pmatrix} \ldots & a & b & c & \ldots & l & m & \ldots \\ \ldots & e & f & g & \ldots & \tau(l) & \tau(m) & \ldots \end{pmatrix}.$$

Dunque possiamo considerare $\overline{\tau} = (\tau(l)\,\tau(m))\tau \in A_n$, avremo come prima

$$(a\,b\,c) = \overline{\tau}(e\,f\,g)\overline{\tau}^{-1}$$

da cui la tesi. □

Teorema 2.7.8. *S_n non è risolubile per $n \geq 5$.*

Dimostrazione. Supponiamo per assurdo che S_n sia risolubile. Allora lo sarà anche $A_n \leq S_n$. Proviamo che A_n non ha sottogruppi normali non banali. In questo modo l'unica catena risolvente per A_n dovrebbe essere $\{(1)\} \leq A_n$, ma A_n non è abeliano quindi ciò sarebbe assurdo.
Sia $\{(1)\} \lneq H \trianglelefteq A_n$, mostriamo che $H = A_n$. Proviamo che in H vi è almeno un 3-ciclo. Sia $\varphi \in H$ con $\varphi \neq (1)$ la sostituzione che lascia fissi il maggior numero possibile di elementi. Supponiamo per assurdo che φ non sia un 3-ciclo. Distinguiamo due casi

1. Nella fattorizzazione di φ in cicli disgiunti compare almeno un ciclo di lunghezza maggiore o uguale a 3. Abbiamo due casi

   (a) φ è un ciclo di lunghezza almeno 5

   $$\varphi = (i\, j\, k\, l\, m \ldots)$$

   (b) φ ha almeno due fattori e uno di essi deve spostare almeno 3 elementi

   $$\varphi = (i\, j\, k \ldots)(l\, m \ldots) \ldots$$

2. φ è prodotto di trasposizioni disgiunte

   $$\varphi = (i\, j)(k\, l) \ldots$$

Poiché $n \geq 5$ allora $\exists m \neq i, j, k, l$. Nei due casi sia $\beta = (k\, l\, m) \in A_n$. Visto che $H \trianglelefteq A_n$ allora $\beta\varphi\beta^{-1} \in H$. Proviamo che $(1) \neq \beta\varphi\beta^{-1}\varphi^{-1} \in H$ lascia fissi più elementi di φ.

1. $\varphi(j) = k, \varphi^{-1}(k) = j$, da cui

   $$\beta\varphi\beta^{-1}\varphi^{-1}(k) = \beta\varphi\beta^{-1}(j) = \beta\varphi(j) = \beta(k) = l \neq k \Rightarrow \beta\varphi\beta^{-1}\varphi^{-1} \neq (1).$$

   Inoltre
   $$\beta\varphi\beta^{-1}\varphi^{-1}(j) = \beta\varphi\beta^{-1}(i) = \beta\varphi(i) = \beta(j) = j,$$
   quindi $\beta\varphi\beta^{-1}\varphi^{-1}$ lascia fissi tutti gli elementi lasciati fissi da φ (e da β) più l'elemnto j, assurdo.

2. $\varphi(k) = \varphi^{-1}(k) = l$, da cui

   $$\beta\varphi\beta^{-1}\varphi^{-1}(k) = \beta\varphi\beta^{-1}(l) = \beta\varphi(k) = \beta(l) = m \neq k \Rightarrow \beta\varphi\beta^{-1}\varphi^{-1} \neq (1).$$

   Inoltre
   $$\beta\varphi\beta^{-1}\varphi^{-1}(j) = \beta\varphi\beta^{-1}(i) = \beta\varphi(i) = \beta(j) = j,$$
   $$\beta\varphi\beta^{-1}\varphi^{-1}(i) = \beta\varphi\beta^{-1}(j) = \beta\varphi(j) = \beta(i) = i,$$
   quindi $\beta\varphi\beta^{-1}\varphi^{-1}$ lascia fissi tutti gli elementi lasciati fissi da φ tranne al più l'elemento m, con l'aggiunta degli elementi i, j, assurdo.

Quindi in H ci sono tutti i coniugati del 3-ciclo, cioè H possiede tutti i 3-cicli. Dal lemma precedente abbiamo $A_n \subseteq H$, cioè $H = A_n$. □

2.8 Estensioni cicliche

Nel seguito supporremo $ch(\mathbb{K}) = 0$.

Definizione 2.8.1. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione finita, con $[\mathbb{K} : \mathbb{F}] = |\mathscr{I}(\mathbb{K}/\mathbb{F})| = n$ (visto che l'estensione è anche separabile in quanto $ch(\mathbb{K}) = 0$) e $\mathscr{I}(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Sia $a \in \mathbb{K}$, si definisce la* ***traccia*** *di a come l'elemento*

$$Tr_{\mathbb{K}/\mathbb{F}}(a) = \sum_{i=1}^{n} \sigma_i(a) \in \overline{\mathbb{F}}.$$

Si definisce la ***norma*** *di a come l'elemento*

$$N_{\mathbb{K}/\mathbb{F}}(a) = \prod_{i=1}^{n} \sigma_i(a) \in \overline{\mathbb{F}}.$$

Proposizione 2.8.2. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di Galois, con $[\mathbb{K} : \mathbb{F}] = |\mathscr{I}(\mathbb{K}/\mathbb{F})| = |\mathcal{G}(\mathbb{K}/\mathbb{F})| = n$ e $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Per ogni $a \in \mathbb{K}$ si ha $Tr_{\mathbb{K}/\mathbb{F}}(a), N_{\mathbb{K}/\mathbb{F}}(a) \in \mathbb{F}$.*

Dimostrazione. L'estensione $\mathbb{F} \subseteq \mathbb{K}$ è di Galois quindi $\mathbb{F} = \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})}$. Sia $a \in \mathbb{K}$, per ogni $\sigma_i \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ abbiamo

$$\sigma_i(Tr_{\mathbb{K}/\mathbb{F}}(a)) = \sigma_i\left(\sum_{j=1}^{n} \sigma_j(a)\right) = \sum_{j=1}^{n} (\sigma_i \circ \sigma_j)(a) = \sum_{j=1}^{n} \sigma_j(a) = Tr_{\mathbb{K}/\mathbb{F}}(a) \in \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$$

$$\sigma_i(N_{\mathbb{K}/\mathbb{F}}(a)) = \sigma_i\left(\prod_{j=1}^{n} \sigma_j(a)\right) = \prod_{j=1}^{n} (\sigma_i \circ \sigma_j)(a) = \prod_{j=1}^{n} \sigma_j(a) = N_{\mathbb{K}/\mathbb{F}}(a) \in \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$$

(nelle penultime uguaglianze abbiamo utilizzato il fatto che gli elementi $\sigma_i \circ \sigma_j$ sono tutti distinti al variare di $j \in \{1, \ldots, n\}$). □

Definizione 2.8.3. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di Galois. Fissiamo una base $\{a_1, a_2, \ldots, a_n\}$ di $\mathbb{K}$ come $\mathbb{F}$-spazio vettoriale. Si definisce* ***discriminante*** *relativo a tale base come*

$$\Delta = \det(\sigma_i(a_j)) = \begin{vmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \ldots & \sigma_1(a_n) \\ \sigma_2(a_1) & \sigma_2(a_2) & \ldots & \sigma_2(a_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \ldots & \sigma_n(a_n) \end{vmatrix}.$$

Proposizione 2.8.4. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione di Galois, con $[\mathbb{K} : \mathbb{F}] = n$, allora $\Delta \neq 0$ e*

$$\Delta^2 = \det(Tr(a_i a_j)) = \begin{vmatrix} Tr(a_1a_1) & Tr(a_1a_2) & \ldots & Tr(a_1a_n) \\ Tr(a_2a_1) & Tr(a_2a_2) & \ldots & Tr(a_2a_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr(a_na_1) & Tr(a_na_2) & \ldots & Tr(a_na_n) \end{vmatrix}$$

Dimostrazione. Sia $A = (\sigma_i(a_j))$ per ogni $i, j \in \{1, \ldots, n\}$. Risulta

$$\Delta^2 = \det(A^t)\det(A) = det(A^t A).$$

Adesso, visto che $A^t = (\sigma_j(a_i))$, ponendo $A^t A = (c_{ij})$ risulta

$$c_{ij} = \sum_{k=1}^{n} \sigma_k(a_i)\sigma_k(a_j) = \sum_{k=1}^{n} \sigma_k(a_i a_j) = Tr(a_i a_j) \Rightarrow \Delta^2 = \det(A^t A) = \det(Tr(a_i a_j)).$$

Sia adesso $T : \mathbb{K} \times \mathbb{K} \to \mathbb{F}$ con $T(a, b) = Tr_{\mathbb{K}/\mathbb{F}}(ab)$. Proviamo che T è una forma bilineare simmetrica. Siano $a, b, c \in \mathbb{K}$ e $\alpha \in \mathbb{F}$

$$T(a + b, c) = Tr_{\mathbb{K}/\mathbb{F}}((a + b)c) = \sum_{i=1}^{n} \sigma_i((a + b)c) =$$

$$= \sum_{i=1}^{n} \sigma_i(ac) + \sigma_i(bc) = Tr_{\mathbb{K}/\mathbb{F}}(ac) + Tr_{\mathbb{K}/\mathbb{F}}(bc) = T(a, c) + T(b, c),$$

$$T(\alpha a, b) = Tr_{\mathbb{K}/\mathbb{F}}(\alpha ab) = \sum_{i=1}^{n} \sigma_i(\alpha ab) = \alpha \sum_{i=1}^{n} \sigma_i(ab) = \alpha Tr_{\mathbb{K}/\mathbb{F}}(ab) = \alpha T(a, b),$$

$$T(a, b) = Tr_{\mathbb{K}/\mathbb{F}}(ab) = Tr_{\mathbb{K}/\mathbb{F}}(ba) = T(b, a).$$

Dunque T è una forma bilineare la cui matrice associata rispetto alla base $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ è $[T]_{\mathcal{A}} = (Tr_{\mathbb{K}/\mathbb{F}}(a_i a_j))$. Poiché per ogni $a \in \mathbb{K} \setminus \{0\}$

$$T(a, a^{-1}) = Tr_{\mathbb{K}/\mathbb{F}}(aa^{-1}) = Tr_{\mathbb{K}/\mathbb{F}}(1) = n \neq 0 \quad (ch(\mathbb{K}) = 0),$$

allora la forma bilineare T è non degenere, ciò è equivalente a $\det([T]_{\mathcal{A}}) \neq 0$, cioè $\det(Tr_{\mathbb{K}/\mathbb{F}}(a_i a_j)) = \Delta^2 \neq 0 \Rightarrow \Delta \neq 0$. □

Osserviamo che ogni automorfismo di $\mathbb{K}$ come campo che lascia fisso $\mathbb{F}$ è anche un automorfismo di $\mathbb{K}$ come $\mathbb{F}$-spazio vettoriale, cioè $\mathcal{G}(\mathbb{K}/\mathbb{F}) \subseteq \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{K})$. Infatti sia $\sigma \in \mathcal{G}(\mathbb{K}/\mathbb{F})$, per ogni $x, y \in \mathbb{K}$ e $a \in \mathbb{F}$ abbiamo

- $\sigma(x + y) = \sigma(x) + \sigma(y)$
- $\sigma(ax) = \sigma(a)\sigma(x) = a\,\sigma(x)$

Adesso definiamo il seguente prodotto

$$f \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{K}),\ \alpha \in \mathbb{K} \quad (\alpha \cdot f)(x) = \alpha\, f(x) \quad \forall x \in \mathbb{K}.$$

Osserviamo che se $f \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{K})$ e $\alpha \in \mathbb{K}$ allora anche $\alpha \cdot f \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{K})$, infatti per ogni $x, y \in \mathbb{K}$ e $a \in \mathbb{F}$ abbiamo

- $(\alpha \cdot f)(x+y) = \alpha f(x+y) = \alpha(f(x)+f(y)) = \alpha f(x)+\alpha f(y) = (\alpha \cdot f)(x)+(\alpha \cdot f)(y)$
- $(\alpha \cdot f)(ax) = \alpha f(ax) = a\alpha f(x) = a(\alpha \cdot f)(x)$

Corollario 2.8.5. *Se l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è di Galois, con $[\mathbb{K} : \mathbb{F}] = n$ e $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathscr{I}(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ allora per ogni n-upla $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n \setminus \{\underline{0}\}$ si ha*

$$\alpha_1\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_n\sigma_n \neq 0_{\mathrm{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{K})}$$

Dimostrazione. Siano $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n$ tale che

$$\alpha_1\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_n\sigma_n = 0_{\mathrm{Hom}_{\mathbb{F}}(\mathbb{K},\mathbb{K})}$$

e $\{a_1, a_2, \ldots, a_n\}$ una base di $\mathbb{K}$ come $\mathbb{F}$-spazio vettoriale. Risulta

$$\begin{cases} \alpha_1\sigma_1(a_1) + \alpha_2\sigma_2(a_1) + \ldots + \alpha_n\sigma_n(a_1) = 0 \\ \alpha_1\sigma_1(a_2) + \alpha_2\sigma_2(a_2) + \ldots + \alpha_n\sigma_n(a_2) = 0 \\ \quad\vdots \qquad\qquad \vdots \qquad\qquad\quad \vdots \\ \alpha_1\sigma_1(a_n) + \alpha_2\sigma_2(a_n) + \ldots + \alpha_n\sigma_n(a_n) = 0 \end{cases}$$

il precedente è un sistema omogeneo con matrice associata $(\sigma_i(a_j))$. Dalla proposizione precedente abbiamo $\det(\sigma_i(a_j)) = \Delta \neq 0$ pertanto $(\alpha_1, \alpha_2, \ldots, \alpha_n) = \underline{0}$. □

Definizione 2.8.6. *Un'estensione $\mathbb{F} \subseteq \mathbb{K}$ di Galois è detta **ciclica** di ordine n se $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è un gruppo ciclico di ordine n.*

Lemma 2.8.7. (Teorema di Hilbert 90) *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione ciclica di ordine n con $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathcal{G}(\tau)$. Se $a \in \mathbb{K}$ allora*

$$N_{\mathbb{K}/\mathbb{F}}(a) = 1 \iff \exists b \in \mathbb{K} : \ a = \frac{b}{\tau(b)}.$$

Dimostrazione.

$\Rightarrow$ Sia

$$\phi = 1 + a \cdot \tau + a\tau(a) \cdot \tau^2 + \ldots + a\tau(a)\ldots\tau^{n-2}(a) \cdot \tau^{n-1} \in \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{K}).$$

ϕ è combinazione lineare a coefficienti in $\mathbb{K}$ non tutti nulli di $\{1, \tau, \ldots, \tau^{n-1}\} = \mathcal{G}(\mathbb{K}/\mathbb{F})$. Dal lemma precedente sappiamo che $\phi \neq \underline{0}$, quindi esiste $c \in \mathbb{K}$ tale che $\phi(c) \neq 0$. Sia

$$b = \phi(c) = c + a\tau(c) + a\tau(a)\tau^2(c) + \ldots + a\tau(a)\ldots\tau^{n-2}(a)\tau^{n-1}(c),$$

si ha

$$\tau(b) = \tau(c) + \tau(a)\tau^2(c) + \tau(a)\tau^2(a)\tau^3(c) + \ldots + \tau(a)\tau^2(a)\ldots\tau^{n-1}(a)\tau^n(c)$$

da cui

$$a\tau(b) = a\tau(c) + a\tau(a)\tau^2(c) + a\tau(a)\tau^2(a)\tau^3(c) + \ldots + a\tau(a)\tau^2(a)\ldots\tau^{n-1}(a)\tau^n(c) =$$
$$= c + a\tau(c) + a\tau(a)\tau^2(c) + a\tau(a)\tau^2(a)\tau^3(c) + \ldots + a\tau(a)\tau^2(a)\ldots\tau^{n-2}(a)\tau^{n-1}(c) = b$$

in quanto $a\tau(a)\tau^2(a)\ldots\tau^{n-1}(a) = N_{\mathbb{K}/\mathbb{F}}(a) = 1$ e $\tau^n = 1$, ottenendo infine $a = \frac{b}{\tau(b)}$.

$\Leftarrow$ Sia $b \in \mathbb{K}$ tale che $a = \frac{b}{\tau(b)}$. Abbiamo

$$\tau(a) = \frac{\tau(b)}{\tau^2(b)} \quad \tau^2(a) = \frac{\tau^2(b)}{\tau^3(b)} \quad \ldots \quad \tau^{n-1}(a) = \frac{\tau^{n-1}(b)}{\tau^n(b)} = \frac{\tau^{n-1}(b)}{b},$$

pertanto

$$N_{\mathbb{K}/\mathbb{F}}(a) = \prod_{i=o}^{n-1} \tau^i(a) = \frac{b}{\tau(b)}\frac{\tau(b)}{\tau^2(b)}\cdots\frac{\tau^{n-2}(b)}{\tau^{n-1}(b)}\frac{\tau^{n-1}(b)}{b} = 1.$$

□

Teorema 2.8.8. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione ciclica di ordine n con $\mathcal{G}(\mathbb{K}/\mathbb{F}) = \mathcal{G}(\tau)$. Se $\mathbb{F}$ contiene le radici primitive n-esime dell'unità allora esiste $b \in \mathbb{K}$ tale che*

1. *$b^n = a \in \mathbb{F}$.*
2. *$\mathbb{K} = \mathbb{F}(b)$.*
3. *$\mathbb{K}$ è campo di spezzamento di $x^n - a \in \mathbb{F}[x]$.*

Dimostrazione. Sia ϵ una radice primitiva n-esima dell'unità, quindi $\epsilon, \epsilon^{-1} \in \mathbb{F}$. Adesso $N_{\mathbb{K}/\mathbb{F}}(\epsilon^{-1}) = (\epsilon^{-1})^n = 1$, dal lemma precedente esiste $b \in \mathbb{K}$ tale che $\epsilon^{-1} = \frac{b}{\tau(b)}$, cioè $\tau(b) = \epsilon b$. Poiché $\tau(b^n) = \tau(b)^n = \epsilon^n b^n = b^n$ allora $b^n = a \in \mathbb{K}^{\mathcal{G}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$ (ogni estensione ciclica è anche di Galois).
Possiamo facilmente dedurre che $\tau^i(b) = \epsilon^i b$ per ogni $i \in \mathbb{N}$, quindi b è lasciato fisso solo da $1_{\mathbb{K}} \in \mathcal{G}(\mathbb{K}/\mathbb{F})$. Consideriamo le estensioni $\mathbb{F} \subseteq \mathbb{F}(b) \subseteq \mathbb{K}$, per la corrispondenza di Galois $\mathbb{F}(b) = \mathbb{K}^H$ con $H \leq \mathcal{G}(\mathbb{K}/\mathbb{F})$. Poiché b è lasciato fisso solo da $1_{\mathbb{K}}$ allora $H = \{1_{\mathbb{K}}\}$, cioè $\mathbb{F}(b) = \mathbb{K}$.
Infine le radici di $x^n - a$ sono $b, \epsilon b, \epsilon^2 b, \dots \epsilon^{n-1} b$. Dunque il campo di spezzamento di $x^n - a$ è $\mathbb{F}(b, \epsilon b, \dots, \epsilon^{n-1} b) = \mathbb{F}(b) = \mathbb{K}$. □

Teorema 2.8.9. *Se $\mathbb{F}$ contiene tutte le radici primitive n-esime dell'unità e $\mathbb{K}$ è il campo di spezzamento di $x^n - a \in \mathbb{F}[x]$, allora*

1. *$\mathbb{F} \subseteq \mathbb{K}$ è di Galois.*
2. *$\mathcal{G}(\mathbb{K}/\mathbb{F})$ è ciclico di ordine $m|n$.*

Dimostrazione. Essendo $\mathbb{K}$ campo di spezzamento di $x^n - a \in \mathbb{F}[x]$, l'estensione $\mathbb{F} \subseteq \mathbb{K}$ è normale, finita e separabile ($ch(\mathbb{K}) = 0$), quindi è di Galois.
Se b è una radice di $x^n - a$ allora $\mathbb{K} = \mathbb{F}(b, \epsilon b, \dots, \epsilon^{n-1} b) = \mathbb{F}(b)$. Siano $\phi_i \in \mathcal{G}(\mathbb{K}/\mathbb{F})$ con $\phi_i(b) = \epsilon^i b$. Sia adesso $\Omega : \mathcal{G}(\mathbb{K}/\mathbb{F}) \to E_n$, dove $E_n = \mathcal{G}(\epsilon)$ è il gruppo moltiplicativo delle radici n-esime dell'unità, con $\Omega(\phi_i) = \epsilon^i$. Ω è chiaramente iniettivo. Proviamo che esso è un omomorfismo di gruppi. Siano $\phi_i, \phi_j \in \mathcal{G}(\mathbb{K}/\mathbb{F})$, si ha

$$(\phi_i \circ \phi_j)(b) = \phi_i(\epsilon^j b) = \epsilon^i \epsilon^j b,$$
$$\Omega(\phi_i \circ \phi_j) = \epsilon^i \epsilon^j = \Omega(\phi_i)\Omega(\phi_j).$$

Dal teorema dell'isomorfismo abbiamo $\mathcal{G}(\mathbb{K}/\mathbb{F}) \simeq \operatorname{Im}\Omega \leq E_n$. Dunque in base al teorema di Lagrange $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è ciclico di ordine $|\mathcal{G}(\mathbb{K}/\mathbb{F})| = m \,|\, n$. □

Corollario 2.8.10. *Se $\mathbb{F}$ è un campo contenente tutte le radici primitive n-esime dell'unità, allora $\mathbb{F} \subseteq \mathbb{K}$ è ciclica di ordine $d|n$ se e solo se esiste $b \in \mathbb{K}$ tale che $b^n = a \in \mathbb{F}$ con $\mathbb{K} = \mathbb{F}(b)$*

Dimostrazione.

⇒ Per ipotesi $d|n$ quindi esiste $\lambda \in \mathbb{N}$ tale che $\lambda d = n$. Dunque se ϵ è una radice primitiva n-esima dell'unità allora $\rho = \epsilon^\lambda$ è una radice primitiva d-esima dell'unità. Pertanto $\mathbb{F}$ contiene tutte le radici d-esime dell'unità, quindi per i teoremi precedenti esiste $b \in \mathbb{K}$ tale che $b^d = a \in \mathbb{F}$, di conseguenza $b^n = b^{\lambda d} = (b^d)^\lambda = a^\lambda \in \mathbb{F}$, e $\mathbb{K} = \mathbb{F}(b)$.

$\Leftarrow$ La tesi segue dal teorema precedente in quanto $\mathbb{K} = \mathbb{F}(b) = \mathbb{F}(b, \epsilon b, \ldots, \epsilon^{n-1}b)$ è campo di spezzamento del polinomio $x^n - a \in \mathbb{F}[x]$

□

Sia $\mathbb{F}$ un campo di caratteristica zero. Consideriamo il polinomio $x^n - a \in \mathbb{F}[x]$ e $b \in \overline{\mathbb{F}}$ una sua radice. Se $\epsilon \in \overline{\mathbb{F}}$ è una radice primitiva n-esima dell'unità allora il campo di spezzamento di $x^n - a$ è

$$\mathbb{K} = \mathbb{F}(b, \epsilon b, \ldots, \epsilon^{n-1}b) = \mathbb{F}(b, \epsilon) \subseteq \overline{\mathbb{F}}.$$

Dunque l'estensione $\mathbb{F} \subseteq \mathbb{F}(b, \epsilon) = \mathbb{K}$ è di Galois, pertanto lo sono anche $\mathbb{F}(b) \subseteq \mathbb{F}(b, \epsilon)$ e $\mathbb{F}(\epsilon) \subseteq \mathbb{F}(b, \epsilon)$. In generale $\mathbb{F} \subseteq \mathbb{F}(b)$ non è di Galois. Un esempio di tale fatto è dato dall'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ che non è di Galois. Invece l'estensione $\mathbb{F} \subseteq \mathbb{F}(\epsilon)$ è di Galois poiché $\mathbb{F}(\epsilon)$ può essere visto come campo di spezzamento del polinomio

$$f_n(x) = \prod_{MCD(n,i)=1} (x - \epsilon^i) \in \mathbb{Z}[x] \subseteq \mathbb{F}[x].$$

Proposizione 2.8.11. *Con le notazioni precedenti, il gruppo $\mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F})$ è risolubile.*

Dimostrazione. Con procedimento analogo a quanto fatto per le estensioni ciclotomiche risulta $\mathcal{G}(\mathbb{F}(\epsilon)/\mathbb{F}) \leq U_n$ abeliano. Consideriamo la catena $\mathbb{F} \subseteq \mathbb{F}(\epsilon) \subseteq \mathbb{F}(b, \epsilon)$. Dato che l'estensione $\mathbb{F} \subseteq \mathbb{F}(\epsilon)$ è di Galois allora dal teorema fondamentale della teoria di Galois

$$\mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F}(\epsilon)) \trianglelefteq \mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F}), \quad \frac{\mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F})}{\mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F}(\epsilon))} \simeq \mathcal{G}(\mathbb{F}(\epsilon)/\mathbb{F}) \leq U_n \text{ abeliano.}$$

Inoltre, applicando il precedente corollario a $\mathbb{F}(\epsilon)$, abbiamo che $\mathcal{G}(\mathbb{F}(\epsilon, b)/\mathbb{F}(\epsilon))$ è ciclico, quindi abeliano. Dunque

$$\{e\} \leq \mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F}(\epsilon)) \leq \mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F})$$

è una catena risolvente per $\mathcal{G}(\mathbb{F}(b, \epsilon)/\mathbb{F})$. □

2.9 Risolubilità di polinomi

Nel seguito supporremo $ch(\mathbb{K}) = 0$.

Definizione 2.9.1. *Un'estensione di campi $\mathbb{F} \subseteq \mathbb{K}$ è detta **radicale** se esiste una catena di campi*

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \ldots \subseteq \mathbb{F}_{n-1} \subseteq \mathbb{F}_n = \mathbb{K}$$

in modo che $\forall i \in \{1, \ldots, n\}$ esistono $\alpha_i \in \mathbb{F}_i$ e $s_i \in \mathbb{N} \setminus \{0\}$ tali che $\mathbb{F}_i = \mathbb{F}_{i-1}(\alpha_i)$ e $\alpha_i^{s_i} \in \mathbb{F}_{i-1}$.

Osservazione 2.9.2. *Ogni estensione radicale è anche finita, infatti la precedente catena di campi è una catena di estensioni semplici e algebriche dato che ogni α_i è algebrico su $\mathbb{F}_{i-1}$ essendo radice del polinomio $x^{s_i} - \alpha_i^{s_i} \in \mathbb{F}_{i-1}[x]$.*

Definizione 2.9.3. *Sia $f(x) \in \mathbb{F}[x]$ un polinomio non costante e sia $\mathbb{L}$ il suo campo di spezzamento. $f(x)$ è detto* ***risolubile per radicali*** *se esiste una estensione radicale $\mathbb{F} \subseteq \mathbb{K}$ tale che $\mathbb{L} \subseteq \mathbb{K}$.*

Lemma 2.9.4. *Se $\mathbb{F} \subseteq \mathbb{K}$ è un'estensione di Galois e ϵ è una radice primitiva n-esima dell'unità allora*

1. *$\mathbb{F}(\epsilon) \subseteq \mathbb{K}(\epsilon)$ è di Galois.*
2. *$\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$ è isomorfo a un sottogruppo di $\mathcal{G}(\mathbb{K}/\mathbb{F})$.*
3. *$\mathcal{G}(\mathbb{K}/\mathbb{F})$ è risolubile $\iff$ $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$ è risolubile.*

Dimostrazione.

1. Per ipotesi $\mathbb{K}$ è campo di spezzamento di qualche polinomio $f(x) \in \mathbb{F}[x]$ separabile. Se pensiamo $f(x) \in \mathbb{F}(\epsilon)[x]$ allora $\mathbb{K}(\epsilon)$ è campo di spezzamento di $f(x) \in \mathbb{F}(\epsilon)[x]$ separabile pertanto $\mathbb{F}(\epsilon) \subseteq \mathbb{K}(\epsilon)$ è di Galois.

2. Sia $\Omega : \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon)) \to \mathcal{G}(\mathbb{K}/\mathbb{F})$ con $\Omega(\varphi) = \varphi_{|\mathbb{K}}$. Ω è un omomorfismo poiché la restrizione della composizione è la composizione delle restrizioni. Inoltre Ω è iniettivo, infatti se $\varphi \in \ker \Omega$ allora $\Omega(\varphi) = \varphi_{|\mathbb{K}} = 1_{\mathbb{K}}$, inoltre essendo $\varphi_{|\mathbb{F}(\epsilon)} = 1_{|\mathbb{F}(\epsilon)}$ allora φ lascia fisso sia $\mathbb{K}$ che ϵ, quindi $\varphi_{|\mathbb{K}(\epsilon)} = 1_{\mathbb{K}(\epsilon)}$. Dunque

$$\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon)) \simeq \operatorname{Im} \Omega \leq \mathcal{G}(\mathbb{K}/\mathbb{F}).$$

3. Osserviamo prima che l'estensione $\mathbb{F} \subseteq \mathbb{K}(\epsilon)$ è di Galois. Infatti per ipotesi $\mathbb{K}$ è campo di spezzamento di un polinomio $f(x) \in \mathbb{F}[x]$, quindi $\mathbb{K}(\epsilon)$ è campo di spezzamento del polinomio $f(x)(x^n - 1) \in \mathbb{F}[x]$, pertanto l'estensione $\mathbb{F} \subseteq \mathbb{K}(\epsilon)$ è finita e normale (ed è anche separabile in quanto $ch(\mathbb{K}) = 0$).
   Inoltre dato che per ipotesi $\mathbb{F} \subseteq \mathbb{K}$ è di Galois e $\mathbb{F} \subseteq \mathbb{F}(\epsilon)$ è di Galois perché estensione ciclotomica, si ha

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) \simeq \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K})},$$
$$\mathcal{G}(\mathbb{F}(\epsilon)/\mathbb{F}) \simeq \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))}.$$

   $\Rightarrow$ Se $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è risolubile allora lo è anche ogni suo sottogruppo. Dal punto 2. abbiamo che $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$ è isomorfo a un sottogruppo di $\mathcal{G}(\mathbb{K}/\mathbb{F})$, quindi è risolubile.

   $\Leftarrow$ $\mathcal{G}(\mathbb{F}(\epsilon)/\mathbb{F}) \leq U_n$ è ciclico, in particolare è abeliano quindi è anche risolubile. Visto che le estensioni $\mathbb{F} \subseteq \mathbb{K}(\epsilon)$ e $\mathbb{F}(\epsilon) \subseteq \mathbb{K}(\epsilon)$ sono di Galois, dal teorema fondamentale della teoria di Galois si ha $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon)) \trianglelefteq \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})$. Dunque, poiché i gruppi

$$\mathcal{G}(\mathbb{F}(\epsilon)/\mathbb{F}) \simeq \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))} \quad \text{e} \quad \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$$

sono risolubili allora da (2.7.4) segue che anche $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})$ è risolubile. Infine, dal momento che

$$\mathcal{G}(\mathbb{K}/\mathbb{F}) \simeq \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F})}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K})}$$

sempre da (2.7.4) segue che $\mathcal{G}(\mathbb{K}/\mathbb{F})$ è risolubile. □

Veniamo adesso a presentare il teorema culmine della teoria di Galois.

Teorema 2.9.5. (Criterio di risolubilità) *Sia $f(x) \in \mathbb{F}[x]$ e $\mathbb{L}$ il suo campo di spezzamento.*

$$f(x) \text{ è risolubile per radicali} \iff \mathcal{G}(\mathbb{L}/\mathbb{F}) \text{ è risolubile.}$$

Dimostrazione. Osserviamo che possiamo supporre $f(x)$ separabile, altrimenti si considera il polinomio $f(x)/MCD(f, f')$. In questo modo l'estensione $\mathbb{F} \subseteq \mathbb{L}$ è di Galois.

$\Rightarrow$ Per ipotesi esiste una catena di estensioni di campi

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_s = \mathbb{K}$$

dove per ogni $i \in \{1, \ldots s\}$ esiste $a_i \in \mathbb{K}_i$ tale che $\mathbb{K}_i = \mathbb{K}_{i-1}(a_i)$ e $a_i^{m_i} \in \mathbb{K}_{i-1}$ per qualche $m_i \in \mathbb{N} \setminus \{0\}$. Inoltre il campo di spezzamento $\mathbb{L}$ di $f(x)$ è contenuto in $\mathbb{K}$. Proviamo che possiamo estendere la precedente catena a un campo $\tilde{\mathbb{K}} \supseteq \mathbb{K}$ tale che $\mathbb{F} \subseteq \tilde{\mathbb{K}}$ sia di Galois. Sia $\mathscr{I}(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_t\}$ e consideriamo la seguente catena

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_s \subseteq \mathbb{K}_{s+1} \subseteq \ldots \subseteq \mathbb{K}_{(t+1)s} = \tilde{\mathbb{K}}$$

dove per ogni $i \in \{1, \ldots, s\}$ e $j \in \{1, \ldots, t\}$ il generico passaggio di tale catena è

$$\mathbb{K}_{js+i} = \mathbb{K}_{js+i-1}(\sigma_j(a_i)).$$

Proviamo che esiste $d \in \mathbb{N} \setminus \{0\}$ tale che $\sigma_j(a_i)^d \in \mathbb{K}_{js+i-1}$. $a_i^{m_i} \in \mathbb{K}_{i-1} = \mathbb{F}(a_1, \ldots, a_{i-1})$, quindi

$$a_i^{m_i} = \sum \beta_{k_1 k_2 \ldots k_i} a_1^{k_1} a_2^{k_2} \ldots a_{i-1}^{k_{i-1}} \in \mathbb{F}(a_1, a_2, \ldots, a_{i-1}) = \mathbb{K}_{i-1}$$

da cui

$$\sigma_j(a_i)^{m_i} = \sum \beta_{k_1 k_2 \ldots k_i} \sigma_j(a_1)^{k_1} \ldots \sigma_j(a_{i-1})^{k_{i-1}} \in \mathbb{F}(\sigma_j(a_1) \ldots \sigma_j(a_{i-1})) \subseteq \mathbb{K}_{js+i-1}.$$

Dunque $f(x)$ è risolubile per radicali anche rispetto all'ultima catena considerata. Proviamo che $\mathbb{F} \subseteq \tilde{\mathbb{K}}$ è di Galois. Prima di tutto osserviamo che l'estensione $\mathbb{F} \subseteq \tilde{\mathbb{K}}$ è finita e separabile (ricordiamo che $ch(\mathbb{F}) = 0$), quindi $\mathbb{F} = \tilde{\mathbb{K}}^{\mathscr{I}(\tilde{\mathbb{K}}/\mathbb{F})}$, pertanto ci basta provare che $\mathscr{I}(\tilde{\mathbb{K}}/\mathbb{F}) = \mathcal{G}(\tilde{\mathbb{K}}/\mathbb{F})$. Essendo $\mathbb{F} \subseteq \tilde{\mathbb{K}}$ algebrica si ha $\mathcal{G}(\tilde{\mathbb{K}}/\mathbb{F}) \subseteq \mathscr{I}(\tilde{\mathbb{K}}/\mathbb{F})$. Sia $\varphi \in \mathscr{I}(\tilde{\mathbb{K}}/\mathbb{F})$, proviamo che φ è un automorfismo di $\tilde{\mathbb{K}}$, per fare ciò basta provare che $\varphi(\sigma_j(a_i)) \in \tilde{\mathbb{K}}$ per ogni $i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\}$. , Ricordando che

$$\mathbb{K} = \mathbb{F}(a_1, a_2, \ldots, a_s) \text{ e che } \tilde{\mathbb{K}} = \mathbb{F}\left(\left\{\sigma_j(a_i) : \begin{array}{c} i = 1, \ldots, s \\ j = 1, \ldots, t \end{array}\right\}\right),$$

poiché $\sigma_j \in \mathscr{I}(\mathbb{K}/\mathbb{F})$ allora la composizione $\varphi \circ \sigma_j$ agisce nel seguente modo

$$\mathbb{K} \xrightarrow{\sigma_j} \tilde{\mathbb{K}} \xrightarrow{\varphi} \overline{\mathbb{F}}$$

quindi anche $\varphi \circ \sigma_j \in \mathscr{I}(\mathbb{K}/\mathbb{F})$, cioè $\varphi \circ \sigma_j = \sigma_h$, per qualche $h = 1, \ldots, t$. Dunque $\varphi(\sigma_j(a_i)) = \sigma_h(a_i) \in \tilde{\mathbb{K}}$ per ogni $i = 1, \ldots, s$, $j = 1, \ldots, t$. Questo prova che $\varphi \in \mathcal{G}(\tilde{\mathbb{K}}/\mathbb{F})$ pertanto $\mathbb{F} \subseteq \tilde{\mathbb{K}}$ è di Galois.
Per quanto dimostrato finora possiamo supporre, a meno di estendere la catena di campi, che $\mathbb{F} \subseteq \mathbb{K}$ sia di Galois. Sia m il minimo comune multiplo di $m_1, m_2, \ldots, m_s$ e sia ϵ una radice primitiva m-esima dell'unità. Per il lemma precedente ci basta dimostrare che $\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{F}(\epsilon))$ è risolubile. Dato che $\mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{F} \subseteq \mathbb{L}$ sono di Galois allora, sempre dal lemma precedente, lo saranno anche $\mathbb{F}(\epsilon) \subseteq \mathbb{K}(\epsilon)$ e $\mathbb{F}(\epsilon) \subseteq \mathbb{L}(\epsilon)$, da cui

$$\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{F}(\epsilon)) \simeq \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{L}(\epsilon))},$$

pertanto è sufficiente dimostrare che $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$ è risolubile. Consideriamo la catena

$$\mathbb{F}(\epsilon) = \mathbb{K}_0(\epsilon) \subseteq \mathbb{K}_1(\epsilon) \subseteq \ldots \subseteq \mathbb{K}(\epsilon).$$

Per ogni $i \in \{1, \ldots, s\}$ si ha $\mathbb{K}_{i-1}(\epsilon)(a_i) = \mathbb{K}_i(\epsilon)$ con $a_i^{m_i} \in \mathbb{K}_{i-1} \subseteq \mathbb{K}_{i-1}(\epsilon)$ e quindi a_i è radice del polinomio $x^{m_i} - a_i^{m_i} \in \mathbb{K}_{i-1}(\epsilon)[x]$. Le altre radici si ottengono moltiplicando a_i per le radici m_i-esime dell'unità che possiamo ottenere a partire da ϵ dal momento che $m_i | m$. Dunque tutte le radici di $x^{m_i} - a_i^{m_i}$ stanno in $\mathbb{K}_i(\epsilon)$, ciò vuol dire che $\mathbb{K}_i(\epsilon)$ è campo di spezzamento di $x^{m_i} - a_i^{m_i} \in \mathbb{K}_{i-1}(\epsilon)[x]$. In questo modo abbiamo provato che l'estensione $\mathbb{K}_{i-1}(\epsilon) \subseteq \mathbb{K}_i(\epsilon)$ è di Galois e inoltre per (2.8.10) $\mathcal{G}(\mathbb{K}_i(\epsilon)/\mathbb{K}_{i-1}(\epsilon))$ è ciclico di ordine un divisore di m_i. Applicando la corrispondenza di Galois alla precedente catena considerata otteniamo una catena di gruppi

$$\{e\} = \Gamma_0 \leq \Gamma_1 \leq \ldots \leq \Gamma_{s-1} \leq \Gamma_s = \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon)),$$

dove $\Gamma_i = \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K}_{s-i}(\epsilon))$ per ogni $i \in \{0, \ldots, s\}$. La precedente è una catena risolvente per $\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{F}(\epsilon))$, infatti per ogni $i \in \{0, \ldots, s-1\}$ si ha

$$\Gamma_i = \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K}_{s-i}(\epsilon)) \trianglelefteq \mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K}_{s-i-1}(\epsilon)) = \Gamma_{i+1},$$

infatti per quanto detto prima $\mathbb{K}_{s-i-1}(\epsilon) \subseteq \mathbb{K}_{s-i}(\epsilon)$ è di Galois e inoltre

$$\frac{\Gamma_{i+1}}{\Gamma_i} = \frac{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K}_{s-i}(\epsilon))}{\mathcal{G}(\mathbb{K}(\epsilon)/\mathbb{K}_{s-i-1}(\epsilon))} \simeq \mathcal{G}(\mathbb{K}_{s-i}(\epsilon)/\mathbb{K}_{s-i-1}(\epsilon)),$$

pertanto Γ_{i+1}/Γ_i è ciclico, quindi abeliano.

$\Leftarrow$ Siano $m = |\mathcal{G}(\mathbb{L}/\mathbb{F})| = [\mathbb{L} : \mathbb{F}]$ ($\mathbb{F} \subseteq \mathbb{L}$ di Galois) e ϵ radice primitiva m-esima dell'unità. Dal lemma precedente sappiamo che l'estensione $\mathbb{F}(\epsilon) \subseteq \mathbb{L}(\epsilon)$ è di Galois e che $\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{F}(\epsilon))$ è isomorfo a un sottogruppo di $\mathcal{G}(\mathbb{L}/\mathbb{F})$. Pertanto $[\mathbb{L}(\epsilon) : \mathbb{F}(\epsilon)] = |\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{F}(\epsilon))|$ divide m. Poniamo $\Gamma = \mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{F}(\epsilon))$. Per il lemma precedente Γ è risolubile, quindi consideriamo una catena risolvente

$$\{e\} = \Gamma_0 \leq \Gamma_1 \leq \ldots \leq \Gamma_{n-1} \leq \Gamma_n = \Gamma$$

con $\Gamma_i \trianglelefteq \Gamma_{i+1}$ e possiamo suppore, in base a (2.7.4), che Γ_{i+1}/Γ_i sia ciclico di ordine un divisore primo di m. Consideriamo la corrispondente catena di sottocampi intermedi

$$\mathbb{F}(\epsilon) = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \mathbb{E}_{n-1} \subseteq \mathbb{E}_n = \mathbb{L}(\epsilon) \tag{2.3}$$

con $\mathbb{E}_i = \mathbb{L}(\epsilon)^{\Gamma_{n-i}}$ per ogni $i \in \{0, \dots n\}$. Scelto un indice $i \in \{0, \dots, n-1\}$ l'estensione $\mathbb{E}_i \subseteq \mathbb{L}(\epsilon)$ è di Galois in quanto lo è $\mathbb{F}(\epsilon) \subseteq \mathbb{L}(\epsilon)$, inoltre

$$\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{E}_{i+1}) = \Gamma_{n-(i+1)} \trianglelefteq \Gamma_{n-i} = \mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{E}_i),$$

pertanto risulta

$$\mathcal{G}(\mathbb{E}_{i+1}/\mathbb{E}_i) \simeq \frac{\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{E}_i)}{\mathcal{G}(\mathbb{L}(\epsilon)/\mathbb{E}_{i+1})} = \frac{\Gamma_{i+1}}{\Gamma_i}.$$

Dunque $\mathcal{G}(\mathbb{E}_{i+1}/\mathbb{E}_i)$ è ciclico di ordine un divisore di m, da cui per definizione l'estensione $\mathbb{E}_i \subseteq \mathbb{E}_{i+1}$ è ciclica di ordine un divisore di m, diciamo m_i. Inoltre $\mathbb{E}_i \supseteq \mathbb{F}(\epsilon)$ contiene tutte le radici primitive m-esime dell'unità. Pertanto, per (2.8.10), esiste $b_i \in \mathbb{E}_{i+1}$ tale che $b_i^{m_i} \in \mathbb{E}_i$ e $\mathbb{E}_{i+1} = \mathbb{E}_i(b_i)$.
In questo modo abbiamo mostrato che l'estensione $\mathbb{F}(\epsilon) \subseteq \mathbb{L}(\epsilon)$ è radicale tramite la catena (2.3). Visto che $\epsilon^m = 1 \in \mathbb{F}$ possiamo allungare tale catena come segue

$$\mathbb{F} \subseteq \mathbb{F}(\epsilon) = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \dots \mathbb{E}_{n-1} \subseteq \mathbb{E}_n = \mathbb{L}(\epsilon)$$

ottenendo che $\mathbb{F} \subseteq \mathbb{L}(\epsilon)$ è ancora un'estensione radicale. Infine, poiché $\mathbb{L} \subseteq \mathbb{L}(\epsilon)$ allora $f(x)$ è risolubile per radicali.

□

Corollario 2.9.6. *Ogni polinomio $f(x) \in \mathbb{F}[x]$ di grado $2, 3$ oppure 4 è risolubile per radicali.*

Dimostrazione. Sia $\mathbb{L}$ il campo di spezzamento di $f(x)$. L'estensione $\mathbb{F} \subseteq \mathbb{L}$ è di Galois (ricordiamo che $ch(\mathbb{F}) = 0$). Dunque $\mathcal{G}(\mathbb{L}/\mathbb{F})$ è isomorfo a un sottgruppo di S_n. Per $n = 2, 3, 4$ sappiamo che S_n è risolubile quindi anche $\mathcal{G}(\mathbb{L}/\mathbb{F})$ è risolubile. Pertanto, alla luce del teorema precedente, $f(x)$ è risolubile per radicali. □

Definizione 2.9.7. *Si dice **polinomio generale** di grado n su $\mathbb{F}$ il polinomio*

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{F}(a_1, \dots, a_n)[x].$$

Lemma 2.9.8. *Ogni funzione razionale di $\mathbb{F}(x_1, \dots, x_n)$ simmetrica si può scrivere sotto forma di funzione razionale nei polinomi simmetrici elementari.*

Dimostrazione. Sia

$$\frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \in \mathbb{F}(x_1, \dots, x_n),$$

con $g(x_1, \dots, x_n) \neq 0$, una funzione razionale simmetrica. Proviamo che esistono due polinomi simmetrici $\bar{f}, \bar{g}$ tali che $f/g = \bar{f}/\bar{g}$. Moltiplichiamo f e g per il prodotto h di tutti gli $n! - 1$ polinomi ottenuti da g scambiando le x_i con tutte le possibili permutazioni

di S_n ad eccezione di quella identica. Il polinomio $\bar{g} = gh$ risulterà così simmetrico. Inoltre anche $\bar{f} = fh$ è simmetrico in quanto

$$fh = (gh)\left(\frac{fh}{gh}\right).$$

□

Teorema 2.9.9. *Il poinomio generale di grado $n \geq 5$ su $\mathbb{F}$ non è risolubile per radicali.*

Dimostrazione. Siano $x_1, x_2, \ldots, x_n$ le radici di $f(x)$. Prima di tutto osserviamo che $\mathbb{F}(a_1, \ldots, a_n) \subseteq \mathbb{F}(x_1, \ldots, x_n)$, infatti i coefficienti a_i di f sono uguali a meno del segno ai polinomi simmetrici elementari calcolati in $x_1, x_2, \ldots, x_n$. Inoltre $\mathbb{F}(x_1, \ldots, x_n)$ è il campo di spezzamento di $f(x)$ su $\mathbb{F}(a_1, \ldots, a_n)$, quindi l'estensione $\mathbb{F}(a_1, \ldots, a_n) \subseteq \mathbb{F}(x_1, \ldots, x_n)$ è di Galois.
Adesso è sufficiente provare che il gruppo di Galois associato all'estensione $\mathbb{F}(a_1, \ldots, a_n) \subseteq \mathbb{F}(x_1, \ldots, x_n)$, è isomorfo a S_n. Per il lemma precedente ogni funzione razionale simmetrica è esprimibile come funzione razionale dei polinomi simmetrici elementari. In altri termini

$$\mathbb{F}(x_1, \ldots, x_n)^{S_n} = \mathbb{F}(\sigma_1, \ldots, \sigma_n) = \mathbb{F}(a_1, \ldots, a_n)$$

$$\mathcal{G}\left(\frac{\mathbb{F}(x_1, \ldots, x_n)}{\mathbb{F}(a_1, \ldots, a_n)}\right) = \mathcal{G}\left(\frac{\mathbb{F}(x_1, \ldots, x_n)}{\mathbb{F}(x_1, \ldots, x_n)^{S_n}}\right) = S_n.$$

□

Lemma 2.9.10. *Per ogni $n \geq 5$ dispari esiste un polinomio $f(x) \in \mathbb{Q}[x]$ irriducibile di grado n che abbia esattamente due radici complesse.*

Dimostrazione. Siano $a_1, \ldots, a_{n-2} \in 2\mathbb{Z}$ tali che $a_1 < a_2 < \ldots < a_{n-2}$ con $\sum_{i=1}^{n-2} a_i = 0$ e sia $c > 1$ un intero pari. Consideriamo $g(x) = (x^2 + c)(x - a_1)\ldots(x - a_{n-2})$. $g(x)$ ha due sole radici complesse $\pm\sqrt{-c}$. Osserviamo che per ogni $i \in \{1, \ldots, n-2\}$ si ha $|g(a_i + 1)| > 2$. Infatti $(a_i + 1)^2 + c > 2$ in quanto $c > 1$ e $a_i \in 2\mathbb{Z}$. Mentre per ogni $j \in \{1, \ldots, n-2\}$ si ha $|a_i + 1 - a_j| \geq 1$. $g(x)$ ha grado dispari, quindi

$$\lim_{x \to \pm\infty} g(x) = \pm\infty.$$

$g(x)$ è continua e derivabile in tutto $\mathbb{R}$, quindi, sapendo che

$$g(a_1) = g(a_2) = \ldots = g(a_{n-2}) = 0$$

in base al teorema di Rolle $g(x)$ ha $\frac{n-3}{2}$ massimi relativi. Da ciò deduciamo che la retta di equazione $y = 2$ interseca $g(x)$ in almeno $n - 3$ punti compresi tra a_1 e a_{n-2}, più un altro punto di intersezione per valori di $x > a_{n-2}$. Sia $f(x) = g(x) - 2$. Per quanto detto finora $f(x)$ ha almeno $n - 2$ radici reali. Inoltre $f(x)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein (ricordiamo che c è pari). Infatti

$$4 \mid -ca_1a_2\ldots a_{n-2} \text{ quindi } 4 \nmid -ca_1a_2\ldots a_{n-2} - 2.$$

Proviamo che a meno di scegliere c sufficientemente grande $f(x)$ non ha altre radici reali oltre le $n-2$ trovate. Risulta

$$f(x) = x^n + \left(-\sum_{i=1}^{n-2} a_i\right) x^{n-1} + \left(c + \sum_{i<j} a_i a_j\right) x^{n-2} + \dots$$

Siano $\alpha_1, \alpha_2, \dots, \alpha_n$ le radici di f. Allora

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n-2} a_i = 0,$$

$$-\frac{1}{2}\sum_{i=1}^{n} \alpha_i^2 = \frac{1}{2}\left(\left(\sum_{i=1}^{n} \alpha_i\right)^2 - \sum_{i=1}^{n} \alpha_i^2\right) = \sum_{i<j} \alpha_i \alpha_j = c + \sum_{i<j} a_i a_j,$$

abbiamo infine

$$\sum_{i=1}^{n} \alpha_i^2 = -2c - 2\sum_{i<j} a_i a_j < 0 \quad \text{per } c >> 0.$$

Dunque $f(x)$ non può avere solo radici reali, pertanto oltre alle $n-2$ radici reali trovate deve avere altre 2 radici complesse coniugate. □

Proposizione 2.9.11. *Per ogni $p \geq 5$ primo esiste $f(x) \in \mathbb{Q}[x]$ irriducibile di grado p tale che $\mathcal{G}(\mathbb{L}/\mathbb{Q}) \simeq S_p$ con $\mathbb{L}$ campo di spezzamento di $f(x)$.*

Dimostrazione. Sia $f(x)$ irriducibile di grado p con $p-2$ radici reali e due complesse non reali. Poiché $f(x)$ è irriducibile allora p divide $[\mathbb{L} : \mathbb{Q}]$, infatti se α è una radice di $f(x)$ allora $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{L}$ con $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ quindi

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}(\alpha)]p.$$

Poiché $|\mathcal{G}(\mathbb{L}/\mathbb{Q})| = [\mathbb{L} : \mathbb{Q}]$, essendo $\mathbb{Q} \subseteq \mathbb{L}$ di Galois, per il teorema di Cauchy esiste un elemento di ordine p in $\mathcal{G}(\mathbb{L}/\mathbb{Q}) \leq S_p$, cioè un p-ciclo. Proviamo che in $\mathcal{G}(\mathbb{L}/\mathbb{Q})$ vi è una trasposizione. Sia $\tau : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ con $\tau(a+ib) = a - ib$. Si ha che $\tau_{|\mathbb{L}} \in \mathcal{G}(\mathbb{L}/\mathbb{Q})$, infatti τ lascia fisse tutte le radici reali di f e scambia le due radici complesse coniugate. Pertanto $\tau_{|\mathbb{L}}$ è una trasposizione e a meno di riordinare gli indici possiamo suppore che $\tau = (1\,2)$. Sia $\sigma \in \mathcal{G}(\mathbb{L}/\mathbb{Q}) \leq S_p$ il p-ciclo, quindi in σ compaiono tutti gli indici da 1 fino a p, allora esiste $h \in \mathbb{N}$ tale che $\sigma^h(1) = 2$. Dunque a meno di scambiare σ con σ^h e di rinominare i rimanenti $p-2$ indici possiamo suppore che $\sigma = (1\,2\,\dots\,p)$. In questo modo otteniamo

$$\sigma^i \tau_{|\mathbb{L}} \sigma^{-i} = \begin{pmatrix} i+1 & i+2 \end{pmatrix} \in \mathcal{G}(\mathbb{L}/\mathbb{Q}),$$

inoltre

$$\begin{pmatrix} i & i+1 \end{pmatrix}\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} i & i+1 \end{pmatrix} = \begin{pmatrix} 1 & i+1 \end{pmatrix}$$

in questo modo otteniamo

$$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}, \dots, \begin{pmatrix} 1 & p \end{pmatrix} \in \mathcal{G}(\mathbb{L}/\mathbb{Q}),$$

infine per ogni i, j tra 1 e p abbiamo

$$\begin{pmatrix} 1 & j \end{pmatrix}\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & j \end{pmatrix} = \begin{pmatrix} i & j \end{pmatrix} \in \mathcal{G}(\mathbb{L}/\mathbb{Q}),$$

quindi $\mathcal{G}(\mathbb{L}/\mathbb{Q}) = S_p$. □

Osservazione 2.9.12. *È possibile provare che questo risultato vale più in generale per ogni $n \geq 5$.*

2.10 Discriminante di un polinomio

Definizione 2.10.1. *Sia $n \geq 2$ e $x_1, x_2, \ldots, x_n$ indeterminate su $\mathbb{F}$. Si chiama* ***discriminante*** *il polinomio*

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{F}[x_1, \ldots, x_n].$$

Osservazione 2.10.2. *Osserviamo subito che il discriminante può essere scritto nel seguente modo*

$$\Delta = (-1)^{\binom{n}{2}} \prod_{i \neq j} (x_i - x_j),$$

da cui deduciamo che il discriminante è un polinomio simmetrico.

Dalla definizione si deduce che il discriminante ha una radice quadrata in $\mathbb{F}[x_1, \ldots, x_n]$.

Definizione 2.10.3. *Definiamo*

$$\sqrt{\Delta} = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Osserviamo che $\sqrt{\Delta}$ non è simmetrico.

Proposizione 2.10.4. *Se $\varphi \in S_n$ allora*

$$\varphi(\sqrt{\Delta}) = sgn(\varphi)\sqrt{\Delta}, \quad con \quad sgn(\varphi) = \begin{cases} 1 & \varphi \in A_n \\ -1 & \varphi \in S_n \setminus A_n \end{cases}$$

(dove con $\varphi(\sqrt{\Delta})$ intendiamo il polinomio $\sqrt{\Delta}$ calcolato in $x_{\varphi(1)}, x_{\varphi(2)}, \ldots, x_{\varphi(n)}$).

Dimostrazione. Basta provare che $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$ se τ è una trasposizione. Supponiamo che $\tau = \begin{pmatrix} i & j \end{pmatrix}$ con $i < j$, allora τ lascia fissi i fattori di $\sqrt{\Delta}$ i cui indici sono diversi da i e j. Se $h > j$ allora $\tau(x_i - x_h) = (x_j - x_h)$ e allo stesso modo $\tau(x_j - x_h) = (x_i - x_h)$. Analogamente avviene nel caso $h < i$. Se invece $i < h < j$ allora $\tau(x_i - x_h) = -(x_h - x_j)$ e $\tau(x_h - x_j) = -(x_i - x_h)$, quindi nel prodotto finale il segno verrà compensato. Infine visto che $\tau(x_i - x_j) = -(x_i - x_j)$ allora $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$, da cui la tesi. □

Per $n = 2, 3$ scriviamo le formule per esprimere Δ in funzione dei σ_i.

$$\begin{array}{ll} n = 2 & \Delta = \sigma_1^2 - 4\sigma_2. \\ n = 3 & \Delta = -4\sigma_2^3 - 27\sigma_3^2 + \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 + 18\sigma_1\sigma_2\sigma_3. \end{array}$$

Definizione 2.10.5. *Sia $f(x) \in \mathbb{F}[x]$ un polinomio, $\mathbb{L}$ il suo campo di spezzamento e $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ le sue radici. Si definisce* ***discriminante*** *di f*

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

e analogamente definiamo

$$\sqrt{\Delta(f)} = \Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)$$

Osservazione 2.10.6. *Dalla definizione segue subito che*

$$\Delta(f) \neq 0 \iff f \text{ è separabile.}$$

Inoltre $\Delta(f)$ non è altro che il polinomio discriminante calcolato nelle radici di f. Essendo il discriminante un polinomio simmetrico, per (1.5.8), abbiamo che $\Delta(f) \in \mathbb{F}$.

Teorema 2.10.7. *Sia $f(x) \in \mathbb{F}[x]$, con $ch(\mathbb{F}) \neq 2$, f separabile e $\mathbb{L}$ il campo di spezzamento di f, allora*

1. *Se $\varphi \in \mathcal{G}(\mathbb{L}/\mathbb{F}) \leq S_n$ allora $\varphi(\sqrt{\Delta(f)}) = sgn(\varphi)\sqrt{\Delta(f)}$.*
2. *$\mathcal{G}(\mathbb{L}/\mathbb{F}) \leq A_n \iff \sqrt{\Delta} \in \mathbb{F}$.*

Dimostrazione.

1. Basta applicare la precedente proposizione su $\sqrt{\Delta}$.
2. $$\sqrt{\Delta(f)} \in \mathbb{F} = \mathbb{L}^{\mathcal{G}(\mathbb{L}/\mathbb{F})} \iff \forall \varphi \in \mathcal{G}(\mathbb{L}/\mathbb{F})\, \varphi(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \iff$$
$$\iff \forall \varphi \in \mathcal{G}(\mathbb{L}/\mathbb{F})\, sgn(\varphi) = 1 \iff \mathcal{G}(\mathbb{L}/\mathbb{F}) \subseteq A_n.$$

□

Corollario 2.10.8. *Sia $f(x) \in \mathbb{F}[x]$ irriducibile e separabile con $\deg f = 3$, $ch(\mathbb{F}) \neq 2$ allora*

$$\begin{aligned} \mathcal{G}(\mathbb{L}/\mathbb{F}) = A_3 &\iff \sqrt{\Delta(f)} \in \mathbb{F} \\ \mathcal{G}(\mathbb{L}/\mathbb{F}) = S_3 &\iff \sqrt{\Delta(f)} \notin \mathbb{F} \end{aligned}$$

Dimostrazione. Si ha $\mathcal{G}(\mathbb{L}/\mathbb{F}) \leq S_3$ e poiché f è irriducibile e $\mathbb{F} \subseteq \mathbb{L}$ è di Galois allora 3 divide $[\mathbb{L} : \mathbb{F}] = |\mathcal{G}(\mathbb{L}/\mathbb{F})|$, quindi, dato che $|S_3| = 6$, $\mathcal{G}(\mathbb{L}/\mathbb{F})$ ha ordine 3 oppure 6, adesso basta applicare il secondo punto del teorema precedente. □

2.11 Formula risolutiva di una cubica

Sia $\mathbb{Q} \subseteq \mathbb{F}$ e supponiamo che $\mathbb{F}$ contenga tutte le radici terze dell'unità. Sia

$$f(x) = x^3 + px + q \in \mathbb{F}[x].$$

I coefficienti p e q sono da considerarsi generici. Dunque, se $\mathbb{L}$ è il campo di spezzamento di f allora $\mathcal{G}(\mathbb{L}/\mathbb{F}) \simeq S_3$, per cui $\sqrt{\Delta(f)} \notin \mathbb{F}$, quindi $\mathbb{F} \subsetneq \mathbb{F}(\sqrt{\Delta(f)}) \subseteq \mathbb{L}$, con $[\mathbb{L} : \mathbb{F}] = 6$ e $[\mathbb{F}(\sqrt{\Delta(f)}) : \mathbb{F}] = 2$, pertanto $[\mathbb{L} : \mathbb{F}(\sqrt{\Delta(f)})] = 3$. Inoltre $\mathbb{F} \subseteq \mathbb{L}$ è di Galois, quindi lo è anche $\mathbb{F}(\sqrt{\Delta(f)}) \subseteq \mathbb{L}$. Dunque $|\mathcal{G}(\mathbb{L}/\mathbb{F}(\sqrt{\Delta(f)}))| = [\mathbb{L} : \mathbb{F}(\Delta(f))] = 3$, cioè

$$\mathcal{G}(\mathbb{L}/\mathbb{F}(\sqrt{\Delta(f)})) \simeq A_3,$$

pertanto $\mathcal{G}(\mathbb{L}/\mathbb{F}(\sqrt{\Delta(f)}))$ è anche ciclico, per (2.8.10) esiste $A \in \mathbb{L}$ tale che $A^3 \in \mathbb{F}(\sqrt{\Delta(f)})$, $\mathbb{F}(\sqrt{\Delta(f)}, A) = \mathbb{L}$ e infine se $\mathcal{G}(\mathbb{L}/\mathbb{F}(\sqrt{\Delta(f)})) = \mathcal{G}(\tau)$ allora

$$\omega^{-1} = \frac{A}{\tau(A)} \quad (\omega \text{ è una radice terza primitiva dell'unità}).$$

Utilizzando lo stesso procedimento di quanto fatto nelle estensioni cicliche sappiamo che, posto

$$\phi = 1 + \omega^{-1}\tau + \omega^{-1}\tau(\omega^{-1})\tau^2,$$

se $c \in \mathbb{L}$ è tale che $\phi(c) \neq 0$ allora $A = \phi(c)$. Siano $\alpha_1, \alpha_2, \alpha_3$ le tre radici distinte di f. Possiamo suppore che $\tau = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$, quindi

$$\phi(\alpha_1) = \alpha_1 + \omega^{-1}\tau(\alpha_1) + \omega^{-1}\tau(\omega^{-1})\tau^2(\alpha_1) = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Sia $\sigma = \begin{pmatrix} 2 & 3 \end{pmatrix} \in \mathcal{G}(\mathbb{L}/\mathbb{F})$. Proviamo che $\phi(\alpha_1) \neq \sigma(\phi(\alpha_1))$. Per assurdo se

$$\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = \phi(\alpha_1) = \sigma(\phi(\alpha_1)) = \alpha_1 + \omega^2\alpha_3 + \omega\alpha_2 \Rightarrow$$

$$\Rightarrow (\omega^2 - \omega)(\alpha_2 - \alpha_3) = 0 \Rightarrow \alpha_2 = \alpha_3, \text{ assurdo.}$$

Dunque $\phi(\alpha_1) \notin \mathbb{L}^{\mathcal{G}(\mathbb{L}/\mathbb{F})} = \mathbb{F}$, quindi dev'essere $\phi(\alpha_1) \neq 0 \in \mathbb{F}$. Ne segue che $A = \phi(\alpha_1) = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$. Inoltre sappiamo che $A^3 \in \mathbb{F}(\sqrt{\Delta(f)})$ quindi $A^3 = c + d\sqrt{\Delta(f)}$ con $c, d \in \mathbb{F}$. Sia $B = \sigma(A) = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$, $B^3 = \sigma(A)^3 = c - d\sqrt{\Delta(f)}$ (σ è una permutazione dispari). Tramite il seguente sistema

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = A \\ \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 = B \end{cases}$$

troviamo le tre radici in funzione di A e B

$$\alpha_1 = \frac{1}{3}(A + B)$$
$$\alpha_2 = \frac{1}{3}(\omega A + \omega^2 B)$$
$$\alpha_3 = \frac{1}{3}(\omega^2 A + \omega B).$$

(si trovano A e B con il procedimento della fotocopia).