

Complementi di Algebra

AlpT (@freaknet.org)

<http://freaknet.org/alpt>

May 6, 2009

Abstract

Questo testo e' una rielaborazione personale degli appunti presi durante il corso di Complementi di Algebra, tenuto dal Prof. Marco D'Anna¹ presso il dipartimento di Matematica, Catania, A.A. 2007/2008.

Saro' ben lieto di correggere ogni eventuale errore che mi comunicherai.

Buon lettura.

~ ~

¹Sito web del Prof. D'Anna: <http://www.dmi.unict.it/~mdanna/>

Copyright ©2008 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1	Preliminari	1
2	Estensione di Campi	8
2.1	Caratteristica	8
2.2	Estensioni	15
2.3	Campi di spezzamento	34
2.4	Campi chiusi e chiusura	42
3	Campi finiti	50
3.1	Proprieta' di $x^{p^n} - x$	55
3.2	Estensioni separabili	58
4	Polinomi simmetrici	69
5	Estensioni normali	74
6	Gruppo di Galois	78
6.1	Teorema fondamentale dell'algebra	107
6.2	Estensioni ciclotomiche	111
6.3	Riga e compasso	119
6.3.1	Ciclotomia	132
7	Gruppi risolubili	139
7.1	Risolubilita' di S_n	145
7.2	Estensioni risolubili	146
7.3	Estensioni risolubili per radicali	158
7.4	Discriminante	166
8	Esercizi	170
9	*	186

1 Preliminari

Utilizzeremo la teoria degli anelli (vedi [AI,17,pg.73]), la teoria dei gruppi (vedi [AII,1,pg.1]) e la teoria degli spazi vettoriali (vedi [AL,3,pg.16]).

Definition 1.1. . Sia A un anello (o gruppo). Se B e' un sottoanello (o sottogruppo) di A , scriveremo $B \leq A$.

Da ora in poi, supporremo che in ogni anello unitario, $0_A \neq 1_A$, ovvero che lo zero dell'anello sia diverso dall'elemento unita', cioe'

$$\{0\} \subset \{0, 1\} \subseteq A$$

Quindi ogni anello unitario ha almeno 2 elementi.

Sia K un campo. Se K' e' un sottocampo di K , scriveremo $K' \preceq K$.

Proposition 1.2. Sia $(A, +, \cdot)$ un anello, allora, $(A, +)$ e' un gruppo. L'elemento neutro e' lo 0.

Proposition 1.3. Sia $(K, +, \cdot)$ un corpo, allora, $(K^*, \cdot)$ e' un gruppo. L'elemento neutro e' 1.

Proposition 1.4. Sia $(K, +, \cdot)$ un campo, allora, $(K^*, \cdot)$ e' un gruppo abeliano.

Proposition 1.5. Sia $K' \subseteq K$ un sottocorpo di K , allora $1_{K'} = 1_K$, ovvero l'elemento unita' di K' coincide con quello di K .

Proof: K'^* , K^* sono dei gruppi rispetto all'operazione $\cdot$, poiche' $K' \subseteq K$, per definizione, K'^* e' un sottogruppo di K^* , e quindi hanno gli stessi elementi unita'. $\square$

Proposition 1.6. Sia K campo, e $K' \subseteq K$, allora

$$K' \preceq K \Leftrightarrow \begin{cases} (K', +) \underset{\text{sotto gruppo}}{\leq} (K, +) \\ (K'^*, \cdot) \underset{\text{sotto gruppo}}{\leq} (K^*, \cdot) \end{cases} \Leftrightarrow \forall a \in K' \begin{cases} 1. a - b \in K' \quad \forall b \in K' \\ 2. ab^{-1} \in K' \quad \forall b \in K' \setminus \{0\} \end{cases}$$

Proof:

(1) Dim. $\Rightarrow$

Per definizione.

(1) Dim. $\Leftarrow$

La 1. assicura che $(K', +)$ e' un sottogruppo di $(K, +)$ (vedi [AII,1.21,pg.7]). Si ha anche che $a - a = 0 \in K'$

La 2. assicura che $(K' \setminus \{0\}, \cdot)$ e' un sottogruppo di $(K^*, \cdot)$ e quindi

$$(K' \setminus \{0\}, \cdot) \underset{\text{sottogruppo}}{\leq} (K^*, \cdot) \Rightarrow \begin{cases} \forall a, b \in K' \quad ab \in K' & (3) \\ 1_K \in K' & (4) \\ \forall b \in K' \quad b^{-1} \in K' & (5) \end{cases}$$

$$(3), 1. \quad \Rightarrow \quad K' \leq K \quad (6)$$

[AI,17.3,pg.77]

(6), (4), (5) $\Rightarrow K'$ e' un sottoanello di K , unitario, in cui tutti gli elementi non nulli sono invertibili
Infine, $\cdot$ e' commutativa in K' , perche' lo e' in K .

Quindi K' e' un sottocampo di K .

□

Definition 1.7. Sia $(a) \trianglelefteq A$ l'ideale generato dall'elemento a . Alcune volte, per evitare confusione, adotteremo la seguente notazione:

$$(a) = \langle a \rangle$$

Proposition 1.8. Sia D un ED (dominio euclideo) e sia $(p) \trianglelefteq D$, $p \neq 0$. Si ha:

$$(p) \text{ massimale} \Leftrightarrow (p) \text{ primo} \Leftrightarrow p \text{ primo} \Leftrightarrow p \text{ irriducibile}$$

Proof: Per il thm [AI,21.10,pg.105], D e' un PID, UFD.

$$\begin{array}{ccccc} p \text{ irriducibile} & \underbrace{\Leftrightarrow} & p \text{ primo} & \underbrace{\Leftrightarrow} & (p) \text{ massimale} \\ & D \text{ UFD, [AI,20.4,pg.96]} & & D \text{ ED, [AI,21.6,pg.99]} & \end{array}$$

□

Proposition 1.9. Sia D un dominio, allora

$$A \leq D \Rightarrow A \text{ dominio}$$

Proof: L'operazione di D e' commutativa in tutto D e quindi in A . Quindi A e' un anello commutativo.

Se per assurdo A avesse divisori dello zero, allora questi sarebbero divisori dello zero di D . Assurdo. □

Proposition 1.10. Siano K un campo, D un dominio e sia $\varphi : D \longrightarrow K$ una immersione, allora,

$$\begin{aligned} f : Q(D) &\longrightarrow K \\ f\left(\frac{a}{b}\right) &= \varphi(a)\varphi(b)^{-1} \end{aligned}$$

e' una immersione, dove $Q(D)$ e' il campo dei quozienti di D .

Proof:

(1) f e' ben definita

Sia $b \in D^*$, allora $\varphi(b) \in D^*$, infatti, se per assurdo $\varphi(b) = 0$, si ha:

$$\varphi(b) = 0 \Rightarrow b \in \ker \varphi \underbrace{=}_{\varphi \text{ e' iniettiva}} \{0\} \Rightarrow b = 0$$

assurdo.

Quindi

$$\begin{cases} \varphi(b) \neq 0 \\ K \text{ campo} \end{cases} \Rightarrow \exists \varphi(b)^{-1} = \frac{1}{\varphi(b)}$$

Ha quindi senso considerare

$$\varphi(a)\varphi(b)^{-1} \in K$$

(2) f e' ben posta

Siano $\frac{a}{b} = \frac{a'}{b'}$, si ha:

$$f\left(\frac{a}{b}\right) = f\left(\frac{a'}{b'}\right) \Leftrightarrow \varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1} \Leftrightarrow \varphi(a)\varphi(b') = \varphi(a')\varphi(b) \Leftrightarrow$$

$$\Leftrightarrow \varphi(ab') = \varphi(a'b) \Leftrightarrow ab' = a'b \Leftrightarrow \frac{a}{b} = \frac{a'}{b'}$$

(3) f e' un omomorfismo

$$\begin{aligned}
f\left(\frac{a}{b} + \frac{a'}{b'}\right) &= f\left(\frac{ab' + a'b}{bb'}\right) = \varphi(ab' + a'b)\varphi(bb')^{-1} = (\varphi(ab') + \varphi(a'b))\varphi(bb')^{-1} = \\
&= \varphi(ab')\varphi(bb')^{-1} + \varphi(a'b)\varphi(bb')^{-1} = \varphi(a)\varphi(b')\varphi(b')^{-1}\varphi(b)^{-1} + \varphi(a')\varphi(b)\varphi(b')^{-1}\varphi(b)^{-1} = \\
&= \varphi(a)\varphi(b)^{-1} + \varphi(a')\varphi(b')^{-1} = f\left(\frac{a}{b}\right) + f\left(\frac{a'}{b'}\right)
\end{aligned}$$

Infine,

$$\begin{aligned}
f\left(\frac{aa'}{bb'}\right) &= \varphi(aa')\varphi(bb')^{-1} = \varphi(a)\varphi(a')\varphi(b)^{-1}\varphi(b')^{-1} = \\
&\underbrace{\varphi(a)\varphi(b)^{-1}\varphi(a')\varphi(b')^{-1}}_{K \text{ e' comm.}} = f\left(\frac{a}{b}\right)f\left(\frac{a'}{b'}\right)
\end{aligned}$$

$$(4) \ker f = \ker \varphi = \{0\}$$

$$\ker f = \left\{ \frac{a}{b} \in Q(D) \mid \varphi(a)\varphi(b)^{-1} = 0 \underbrace{\Leftrightarrow}_{\varphi(b) \neq 0} \varphi(a) = 0 \Leftrightarrow a \in \ker \varphi = \{0\} \Leftrightarrow a = 0 \right\} = \{0\}$$

$$\ker f = \{0\} \Rightarrow f \text{ iniettiva}$$

□

Proposition 1.11. $Q(D)$ e' il piu' piccolo campo tale che $D \hookrightarrow Q(D)$, ovvero e' il piu' piccolo campo che contiene per immersione D , o ancora, preso un generico campo K , si ha

$$D \hookrightarrow K \Rightarrow Q(D) \hookrightarrow K$$

*Nota*².

Proof:

$$D \hookrightarrow K \Leftrightarrow \exists \varphi : D \longrightarrow K \text{ omomorfismo iniettivo}$$

Allora basta applicare la prop [1.10,pg.2]

□

Proposition 1.12. Sia K un campo, allora

$$Q(K) \simeq K$$

Proof: Usando l'identita' $i : K \longrightarrow K$, e applicando la [1.10,pg.2], abbiamo che

$$f : Q(K) \longrightarrow K$$

$$f\left(\frac{a}{b}\right) = ab^{-1}$$

e' una immersione. E' anche surriettiva, infatti, preso $c \in K$,

$$f\left(\frac{c}{1}\right) = c$$

quindi $Q(K) \simeq K$.

□

Proposition 1.13. Sia K, K' due campi $\varphi : K \longrightarrow K'$ un omomorfismo tra essi. L'applicazione

$$\tilde{\varphi} : K[x] \longrightarrow K'[x]$$

$$\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \varphi(a_i) x^i$$

si chiama omomorfismo indotto da φ .

$\tilde{\varphi}$ e' un omomorfismo. Se φ e' iniettivo o surriettivo, anche $\tilde{\varphi}$ lo e'.

²con $A \hookrightarrow B$, intendiamo che esiste un omomorfismo iniettivo da A a B

Proof:

(1) $\tilde{\varphi}$ e' un omomorfismo

Siano $\sum_{i=0}^n a_i x^i, \sum_{i=0}^m b_i x^i \in K[x]$, di grado n, m . Ponendo

$$a_{n+i} = b_{m+i} = 0 \quad \forall i = 1, 2, \dots$$

si ha

$$\begin{aligned} \varphi(a_{n+i}) &= \varphi(b_{m+i}) = 0 \quad \forall i = 1, 2, \dots \quad (*) \\ \sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i &= \sum_{i=1}^{\max\{m,n\}} (a_i + b_i) x^i \mapsto \sum_{i=1}^{\max\{m,n\}} \varphi(a_i + b_i) x^i = \\ &= \sum_{i=1}^{\max\{m,n\}} (\varphi(a_i) + \varphi(b_i)) x^i \stackrel{(*)}{=} \sum_{i=0}^n \varphi(a_i) x^i + \sum_{i=0}^m \varphi(b_i) x^i \end{aligned}$$

Analogamente per il prodotto:

$$\begin{aligned} \sum_{i=0}^n a_i x^i \cdot \sum_{i=0}^m b_i x^i &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i \mapsto \sum_{i=0}^{n+m} \varphi \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i = \\ &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^i \varphi(a_j) \varphi(b_{i-j}) \right) x^i = \sum_{i=0}^n \varphi(a_i) x^i \cdot \sum_{i=0}^m \varphi(b_i) x^i \end{aligned}$$

(2) φ iniettiva $\Rightarrow \tilde{\varphi}$ iniettiva

$$\varphi \text{ iniettiva} \Leftrightarrow \ker \varphi = \{0\} \quad (*)$$

$$\ker \tilde{\varphi} = \left\{ \sum_{i=0}^n a_i x^i \mid \sum_{i=0}^n \varphi(a_i) x^i \equiv 0 \Leftrightarrow \varphi(a_i) = 0 \quad \forall i \Leftrightarrow a_i \in \ker \varphi \quad \forall i \stackrel{(*)}{\Leftrightarrow} a_i = 0 \quad \forall i \Leftrightarrow \sum_{i=0}^n a_i x^i \equiv 0 \right\} = \{0\}$$

(3) φ surriettiva $\Rightarrow \tilde{\varphi}$ surriettiva

$$\begin{aligned} \sum_{i=1}^n b_i x^i \in K'[x] &\Rightarrow b_i \in K'[x] \quad \underbrace{\Rightarrow}_{\varphi \text{ surriettiva}} \exists a_i \in K[x] : \varphi(a_i) = b_i \\ &\Rightarrow \sum_{i=1}^n b_i x^i = \sum_{i=1}^n \varphi(a_i) x^i = \tilde{\varphi} \left(\sum_{i=1}^n a_i x^i \right) \end{aligned}$$

□

Definition 1.14. Sia K un campo e $K[x]$ il dominio euclideo dei polinomi a coefficienti in K .
 Preso un

$$f(x) = a_0 + a_1 x + \dots + a_n x^n = \sum_{i=0}^n a_i x^i \in K[x]$$

definiamo la sua derivata:

$$f'(x) \stackrel{\text{def}}{=} a_1 + 2a_2 x + \dots + na_n x^{n-1} = \sum_{i=1}^n i a_i x^{i-1} \in K[x]$$

Dove l'operazione $i a_i$ e':

$$i a_i = \underbrace{a_i + a_i + \dots + a_i}_{i \text{ volte}}$$

Attenzione: questa nozione di derivata coincide con quella analitica solo per opportuni campi K .

Nota³

Proposition 1.15. *Valgono le usuali proprietà della derivata:*

1. $D[f(x) + g(x)] = f'(x) + g'(x)$
2. $D[f(x)g(x)] = f'(x)g(x) + f(x)g'(x)$
3. $D[f(x)^n] = n f(x)^{n-1} f'(x)$
4. $D[f(g(x))] = f'(g(x))g'(x)$

Proof: Siano

$$f(x) = \sum_{i=0}^n a_i x^i$$

$$g(x) = \sum_{i=0}^m b_i x^i$$

(1) Dim 1.

$$D[f(x) + g(x)] = D \left[\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i \right] = \sum_{i=1}^n i a_i x^{i-1} + \sum_{i=1}^m i b_i x^{i-1} = f'(x) + g'(x)$$

(2) Dim 3.

Per induzione su n :

$$\begin{aligned} D[f(x)^n] &= D[f(x)f(x)^{n-1}] \underset{2.}{=} f'(x)f(x)^{n-1} + f(x)D[f(x)^{n-1}] = \\ &\underset{\text{Hp indutt.}}{=} f'(x)f(x)^{n-1} + (n-1)f(x)f(x)^{n-2}f'(x) = \\ &= f'(x)(f(x)^{n-1} + (n-1)f(x)f(x)^{n-2}) = \\ &= f'(x)(f(x)^{n-1} + (n-1)f(x)^{n-1}) = n f'(x)(f(x)^{n-1}) \end{aligned}$$

(3) Dim 4.

³In realta', l'operazione ia_i coincide con l'operazione di moltiplicazione del campo K . Vedi [2.12,pg.14]

$$\begin{aligned}
D[f(g(x))] &= D\left[\sum_{i=0}^n a_i g(x)^i\right] \underset{1.}{=} \sum_{i=0}^n D[a_i g(x)^i] = \\
&\underset{2.}{=} \sum_{i=0}^n a_i D[g(x)^i] = \\
&= a_0 D[g(x)^0] + \sum_{i=1}^n a_i D[g(x)^i] = \\
&= \underbrace{a_0 D[1]}_{=0} + \sum_{i=1}^n a_i D[g(x)^i] = \\
&= \sum_{i=1}^n a_i D[g(x)^i] = \\
&\underset{3.}{=} \sum_{i=1}^n i a_i g(x)^{i-1} g'(x) = \\
&= g'(x) \sum_{i=1}^n i a_i g(x)^{i-1} = g'(x) f'(g(x))
\end{aligned}$$

□

Proposition 1.16.

$$g'(x) \equiv 0 \vee \deg g'(x) < \deg g(x)$$

Proof: Segue immediatamente dalla definizione di derivata.

NB: dobbiamo distinguere i due casi perche' il polinomio nullo non ha grado! □

Proposition 1.17. Sia $f(x) \in K[x]$, e sia α una radice di $f(x)$, ovvero, $f(\alpha) = 0$, allora si ha

$$\mu_f(\alpha) > 1 \Leftrightarrow f'(\alpha) = 0$$

dove con $\mu_f(\alpha)$ abbiamo indicato la molteplicita' della radice α di f .

Nota: se $\mu_f(\alpha) > 1$, allora α viene chiamata radice multipla, altrimenti, se $\mu_f(\alpha) = 1$, radice semplice.

Proof:

(1) Dim. $\Rightarrow$

$$m = \mu_f(\alpha) > 1 \underset{\text{thm di Ruffini [AI, 16.1, pg. 66]}}{\Rightarrow} f(x) = (x - \alpha)^m g(x), \quad g(\alpha) \neq 0$$

$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x) \Rightarrow f'(\alpha) = 0$$

(1) Dim. $\Leftarrow$

Sempre per Ruffini,

$$f(x) = (x - \alpha)g(x), \quad g(\alpha) \neq 0$$

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

$$f'(\alpha) \underset{\text{Hp}}{=} 0 \Leftrightarrow g(\alpha) + g'(\alpha)(\alpha - \alpha) = 0 \Leftrightarrow g(\alpha) = 0 \Rightarrow g(x) = (x - \alpha)h(x)$$

$$f(x) = (x - \alpha)^2 h(x) \Rightarrow \mu_f(\alpha) \geq 2 > 1$$

□

Definition 1.18. Sia V un K -spazio vettoriale. Con il simbolo:

$$\mathcal{L}(v_1, v_2, \dots, v_m)_K$$

oppure con

$$B = \{v_1, \dots, v_m\}$$

$$\mathcal{L}(B)_K$$

indichiamo il K -sottospazio vettoriale di V , generato da $\{v_1, v_2, \dots, v_m\}$.

Proposition 1.19. Sia $f(x) = x^n - a \in \mathbb{C}[x]$, con $a \neq 0$. Tutte e sole le radici di $f(x)$ sono

$$\sqrt[n]{a}, \sqrt[n]{a}\omega, \sqrt[n]{a}\omega^2, \dots, \sqrt[n]{a}\omega^{n-1}$$

dove ω e' una qualsiasi radice dell'unita' che genera $(U_n, \cdot)$ (il gruppo delle radici n -esime dell'unita'), ovvero $U_n = \langle \omega \rangle$.

Proof:

$$x^n - a = 0 \underset{a \neq 0}{\Leftrightarrow} \frac{x^n}{a} - 1 = 0 \Leftrightarrow \left(\frac{x}{\sqrt[n]{a}} \right)^n - 1 = 0 \underset{y = \frac{x}{\sqrt[n]{a}}}{\Leftrightarrow} y^n - 1 = 0$$

Per definizione, tutte le radici di $y^n - 1$ sono gli elementi di U_n , cioe'

$$U_n = \langle \omega \rangle = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$$

Quindi

$$\frac{x}{\sqrt[n]{a}} = y = 1, \omega, \omega^2, \dots, \omega^{n-1} \Leftrightarrow x = \sqrt[n]{a}, \sqrt[n]{a}\omega, \sqrt[n]{a}\omega^2, \dots, \sqrt[n]{a}\omega^{n-1}$$

□

Proposition 1.20. Consideriamo il polinomio $x + y \in \mathbb{Z}_n[x, y]$, si ha

$$(x + y)^n = x^n + y^n$$

Proof:

$$(x + y)^n \underset{\text{binom. Newton}}{=} \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} =$$

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \Rightarrow n / \binom{n}{i} \quad \forall i = 1, \dots, n-1 \Rightarrow \binom{n}{i} = 0 \quad \mathbb{Z}_n \quad \forall i = 1, \dots, n-1$$

$$= x^0 y^{n-0} + x^n y^0 = x^n + y^n$$

□

Definition 1.21. Lemma di Zorn.

Sia $A \neq \emptyset$ un POSET,

ogni catena di elementi di A possiede un maggiorante in $A \Rightarrow A$ possiede elementi massimali

Il lemma di Zorn e' equivalente all'assioma della scelta.

2 Estensione di Campi

2.1 Caratteristica

Proposition 2.1. *Sia A un anello unitario, e sia data la seguente funzione:*

$$\gamma : \mathbb{Z} \longrightarrow A$$

$$\gamma(z) = \begin{cases} z * 1_A & z > 0 \\ 0 & z = 0 \\ -((-z) * 1_A) & z < 0 \end{cases}$$

dove 1_A e' l'unita' di A , e

$$n * a \stackrel{\text{def}}{=} \underbrace{a + a + \cdots + a}_{a \text{ volte}}$$

Si ha che $\gamma(z)$ e' un omomorfismo, inoltre $\gamma(1) = 1_A$.

Proof: Dobbiamo dimostrare che $\forall m, n \in \mathbb{Z}$, si ha

$$\gamma(m+n) = \gamma(m) + \gamma(n)$$

$$\gamma(mn) = \gamma(m)\gamma(n)$$

CASE: $m, n > 0$

$$\gamma(m+n) = (m+n) * 1_A = m * 1_A + n * 1_A$$

CASE: $m > 0, n < 0$

$$\gamma(m) = m * 1_A \qquad \gamma(n) \stackrel{\underbrace{=}_{n < 0}}{=} -(-n) * 1_A$$

CASE: $m+n = 0$

$$m+n = 0 \Leftrightarrow m = -n$$

$$\gamma(m+n) = \gamma(0) = 0$$

$$\gamma(m) + \gamma(n) = m * 1_A - (-n) * 1_A = \underbrace{(1_A + 1_A + \cdots + 1_A)}_{m \text{ volte}} - \underbrace{(1_A + 1_A + \cdots + 1_A)}_{-n \text{ volte}} \stackrel{\underbrace{=}_{m=-n}}{=} 0 = \gamma(m+n)$$

CASE: $m+n > 0$

$$m+n > 0 \Leftrightarrow m > -n$$

$$\gamma(m+n) = (m+n) * 1_A$$

$$\gamma(m) + \gamma(n) = m * 1_A - (-n) * 1_A = \underbrace{(1_A + 1_A + \cdots + 1_A)}_{m \text{ volte}} - \underbrace{(1_A + 1_A + \cdots + 1_A)}_{-n \text{ volte}} =$$

$$\stackrel{\underbrace{=}_{m > -n}}{(m - (-n)) * 1_A} = (m+n) * 1_A = \gamma(m+n)$$

CASE: $m+n < 0$

$$m + n < 0 \Leftrightarrow m < -n$$

$$\gamma(m + n) = -(-n - m) * 1_A$$

$$\begin{aligned} \gamma(m) + \gamma(n) &= m * 1_A - (-n) * 1_A = \underbrace{(1_A + 1_A + \dots + 1_A)}_{m \text{ volte}} - \underbrace{(1_A + 1_A + \dots + 1_A)}_{-n \text{ volte}} = \\ &\stackrel{m < -n}{=} -(-n - m) * 1_A = \gamma(m + n) \end{aligned}$$

CASE: $m < 0, n > 0$

Analogamente a prima.

CASE: $m, n < 0$

$$m + n < 0$$

$$\gamma(m + n) = -(-m - n) * 1_A$$

$$-(-m) * 1_A - (-n) * 1_A = -(-m - n) * 1_A$$

Infine,

CASE: $mn = 0$

$$mn = 0 \Leftrightarrow m = 0 \vee n = 0 \Rightarrow \gamma(m) = 0 \vee \gamma(n) = 0 \quad (1)$$

$$\gamma(mn) = 0 \stackrel{(1)}{=} \gamma(m)\gamma(n)$$

CASE: $mn > 0$

$$\gamma(mn) = (mn) * 1_A$$

$$\gamma(m)\gamma(n) = m * 1_A n * 1_A = m * 1_A \underbrace{(1_A + 1_A + \dots + 1_A)}_{n \text{ volte}} = m * 1_A + m * 1_A + \dots + m * 1_A = (nm) * 1_A$$

CASE: $mn < 0$

$$mn < 0 \Rightarrow m < 0 \text{ XOR } n < 0 \Rightarrow \gamma(m) = (-m) * 1_A \text{ XOR } \gamma(n) = (-n) * 1_A$$

$$\gamma(mn) = -(-mn) * 1_A$$

$$\begin{aligned} \gamma(m) &= (-m) * 1_A \Rightarrow \gamma(m)\gamma(n) = -(-m) * 1_A n * 1_A = -(-m) * 1_A \underbrace{(1_A + 1_A + \dots + 1_A)}_{n \text{ volte}} = \\ &= -((-m) * 1_A + (-m) * 1_A + \dots + (-m) * 1_A) = -(-nm) * 1_A = \gamma(mn) \end{aligned}$$

□

Definition 2.2. Sia dato un anello unitario A , e sia γ la funzione definita in [2.1,pg.8], definiamo la *caratteristica* di A :

$\text{ch}A$ e' il generatore non negativo di $\ker \gamma$, ovvero

$$\ker \gamma \stackrel{\text{def}}{=} (\text{ch}A) = \{\lambda \text{ch}A \mid \lambda \in \mathbb{Z}\}, \quad \text{ch}A \in \mathbb{Z}_+$$

Questa definizione ha senso:

tutti gli ideali di $\mathbb{Z}$ sono PID del tipo (z) , [vedi [AI,18.8,pg.93]] (1)

$$\begin{cases} \ker \gamma \trianglelefteq \mathbb{Z} \\ (1) \end{cases} \Rightarrow \exists z \in \ker \gamma : \ker \gamma = (z)$$

Se poi $z \geq 0$, allora z e' unico: infatti, presi $z_1, z_2 \geq 0 : \ker \gamma = (z_1) = (z_2)$, si ha

$$\begin{aligned} z_1 \in (z_2) &\Rightarrow z_1 = \lambda z_2 \Leftrightarrow z_2 \Big/ z_1 \\ z_2 \in (z_1) &\Rightarrow z_2 = \lambda' z_1 \Leftrightarrow z_1 \Big/ z_2 \\ &\Rightarrow z_1 = z_2 \end{aligned}$$

Quindi, il generatore non negativo di $\ker \gamma$ e' unico.

Proposition 2.3. *Sia A un anello unitario, e sia dato il seguente insieme⁴:*

$$A_0 = \{r \in \mathbb{Z}_+^* \mid r * A = \{0\}\}$$

dove $r * A = \{ra \mid a \in A\}$. Si ha,

$$\text{ch}A = \begin{cases} \min A_0 & A_0 \neq \emptyset \\ 0 & A_0 = \emptyset \end{cases}$$

Proof:

(1) Dim. che $\mathbb{Z}_+^* \cap \ker \gamma = A_0$

Sia $k \in \mathbb{Z}_+^* \cap \ker \gamma$,

$$k \in \mathbb{Z}_+^* \cap \ker \gamma \Leftrightarrow \begin{cases} k \in \ker \gamma \subseteq \mathbb{Z} \\ k > 0 \end{cases}$$

$$k \in \ker \gamma \Rightarrow \gamma(k) = 0 \Leftrightarrow \underbrace{k * 1_A}_{k>0} = 0$$

$$\text{Sia } a \in A, \quad \underbrace{(k * 1_A)a}_{=0} = 0 \Leftrightarrow k * a = 0 \quad \forall a \in A \Rightarrow k \in A_0$$

Sia adesso, $r \in A_0$,

$$r \in A_0 \Rightarrow r > 0, r * 1_A = 0 \Rightarrow \gamma(r) = 0 \Rightarrow r \in \ker \gamma$$

$$r > 0, r \in \ker \gamma \Rightarrow r \in \mathbb{Z}_+^* \cap \ker \gamma$$

CASE: $A_0 = \emptyset$

$$\mathbb{Z}_+^* \cap \ker \gamma \subseteq A_0 = \emptyset \Rightarrow \mathbb{Z}_+^* \cap \ker \gamma = \emptyset \Leftrightarrow \mathbb{Z}_+ \cap \ker \gamma \setminus \{0\} = \emptyset \xRightarrow{0 \in \mathbb{Z}_+ \cap \ker \gamma} \mathbb{Z}_+ \cap \ker \gamma = \{0\} \quad (1)$$

Si ha anche che $\mathbb{Z}_- \cap \ker \gamma = \{0\}$, infatti, se per assurdo $\exists z \in \ker \gamma : z < 0$, allora

$$z < 0 \Leftrightarrow -z > 0 \Leftrightarrow -z \in \mathbb{Z}_+$$

$$z \in \ker g \Leftrightarrow \gamma(z) = 0 \Leftrightarrow -\gamma(z) = 0 \Leftrightarrow \gamma(-z) = 0 \Leftrightarrow -z \in \ker g$$

$$\Rightarrow -z \in \mathbb{Z}_+ \cap \ker \gamma \xRightarrow{(1)} -z = 0 \text{ assurdo contro } z < 0$$

In conclusione:

$$\begin{cases} \ker \gamma \subseteq \mathbb{Z} \\ \mathbb{Z}_+ \cap \ker \gamma = \{0\} = \mathbb{Z}_- \cap \ker \gamma \\ \mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_- \end{cases} \Rightarrow \ker \gamma = \{0\}$$

Quindi,

$$A_0 = \emptyset \Rightarrow \ker \gamma = \{0\} \Leftrightarrow \ker \gamma = (0) \Leftrightarrow \text{ch}A = 0$$

⁴abbiamo posto: $\mathbb{Z}_+ = \{z \in \mathbb{Z} \mid z \geq 0\}$, $\mathbb{Z}_+^* = \mathbb{Z}_+ \setminus \{0\}$

CASE: $A_0 \neq \emptyset$

$$\begin{aligned}\mathbb{Z}_+^* \cap \ker \gamma &= A_0 \neq \emptyset \Rightarrow \ker \gamma \neq \emptyset \Rightarrow \ker \gamma = (\text{ch}A) \neq \{0\} \Rightarrow \text{ch}A > 0 \\ \text{ch}A &\in (\text{ch}A) = \ker \gamma \\ \text{ch}A &> 0 \\ &\Rightarrow \text{ch}A \in \mathbb{Z}_+^* \cap \ker \gamma \subseteq A_0\end{aligned}$$

Sia $m = \min A_0$,

$$\begin{aligned}\text{ch}A \in A_0 &\Rightarrow m \leq \text{ch}A \\ m \in A_0 \supseteq \mathbb{Z}_+^* \cap \ker \gamma &\Rightarrow m \in (\text{ch}A) \Rightarrow m = \lambda \text{ch}A \\ m, \text{ch}A > 0 &\Rightarrow \lambda > 0 \Rightarrow \text{ch}A \leq m \\ \begin{cases} m \leq \text{ch}A \\ m \geq \text{ch}A \end{cases} &\Rightarrow m = \text{ch}A\end{aligned}$$

□

Proposition 2.4. *Sia A un anello unitario e sia dato il seguente insieme:*

$$A_1 = \{r \in \mathbb{Z}_+^* \mid r * 1 = 0\}$$

allora

$$\text{ch}A = \begin{cases} \min A_1 & A_1 \neq \emptyset \\ 0 & A_1 = \emptyset \end{cases}$$

Proof: Sia $c = \text{ch}A$. Sfruttiamo la prop [2.3,pg.10]

CASE: $A_0 = \emptyset$

Dimostriamo che anche $A_1 = \emptyset$. Se per assurdo $r \in A_1$, allora

$$r * 1 = 0 \Rightarrow (r * 1)a = 0 \quad \forall a \in A \Leftrightarrow (1 + 1 + \dots + 1)a = 0 \quad \forall a \Leftrightarrow a + a + \dots + a = 0 \quad \forall a \Leftrightarrow r * a = 0 \Rightarrow r \in A_0 \quad (1)$$

assurdo contro $A_0 \neq \emptyset$.

(1) $A_0 \neq \emptyset$

Per la prop [2.3,pg.10], $c = \text{ch}A = \min A_0$,

$$\begin{aligned}c * A &= \{0\} \Leftrightarrow c * a = 0 \quad \forall a \in A \Leftrightarrow \\ &\Leftrightarrow a + a + \dots + a = 0 \quad \forall a \in A \quad \underbrace{\Leftrightarrow}_{A \text{ e' unitario}} (1 + 1 + \dots + 1)a = 0 \quad \forall a \in A \Leftrightarrow \\ &\Leftrightarrow (c * 1)a = 0 \quad \forall a \in A\end{aligned}$$

In particolare, per $a = 1$, abbiamo $c * 1 = 0 \Rightarrow c \in A_1$

Resta da dimostrare che $c \leq r \quad \forall r \in A_1$. Sia $r \in A_1$, allora

$$r * 1 = 0 \underbrace{\Rightarrow}_{(1)} r \in A_0 \Rightarrow c = \min A_0 \leq r$$

Quindi $c = \min A_1$.

□

Definition 2.5. Sia D un dominio e sia dato il seguente insieme:

$$D_0 = \{r \in \mathbb{Z}_+^* \mid r * D = \{0\}\}$$

Definiamo la caratteristica di D :

$$\text{ch}D = \begin{cases} \min D_0 & D_0 \neq \emptyset \\ 0 & D_0 = \emptyset \end{cases}$$

Per quanto abbiamo visto in [2.3,pg.10], se D e' unitario, possiamo considerare l'omomorfismo $\gamma : \mathbb{Z} \longrightarrow D$, e le due definizioni date di $\text{ch}D$ coincidono.

Lemma 2.6. *Dato un anello A e $r, s \in \mathbb{Z}_+^*$ si ha*

$$rs * (d_1 d_2) = (r * d_1)(s * d_2)$$

Proof:

$$rs * (d_1 d_2) = (rs * d_1)d_2 = (s * (r * d_1))d_2 = s * (d_2(r * d_1)) = (r * d_1)(s * d_2)$$

□

Proposition 2.7. *Si ha:*

$$D \text{ dominio} \Rightarrow \text{ch}D = 0 \vee \text{ch}D = 1 \vee \text{ch}D = p$$

$$D \text{ dominio unitario} \Rightarrow \text{ch}D = 0 \vee \text{ch}D = p$$

con p primo.

Proof: Supponiamo che $\text{ch}D \neq 0$ e dimostriamo che $\text{ch}D = p$.

Se $\text{ch}D = 1$, allora non abbiamo nulla da dimostrare. Supponiamo quindi $\text{ch}D \neq 1$ e supponiamo per assurdo che $\text{ch}D = rs$, con $r, s \neq 1$, allora:

$$rs * d = 0 \quad \forall d \in D \Rightarrow rs * (d') = 0, \text{ con } d' = dd, \quad \forall d \in D$$

$$rs * (dd) = 0 \quad \underbrace{\Leftrightarrow}_{[2.6, \text{pg.12}]} (r * d)(s * d) = 0 \quad \underbrace{\Rightarrow}_{D \text{ dominio d'integrit\`a}} r * d = 0 \vee s * d = 0 \quad \forall d \in D \quad (1)$$

(1) Dim. che

$$\forall d \in D \quad r * d = 0 \quad \vee \quad \forall d \in D \quad s * d = 0$$

ovvero: $r * d = 0$ per tutte le d , oppure $s * d = 0$ per tutte le d . (OR inclusivo)

Se $\forall d \in D \quad r * d = s * d = 0$, non abbiamo nulla da dimostrare. Supponiamo allora che $\exists d \in D^* : r * d \neq 0, s * d = 0$. Si ha:

$$r * d \neq 0 \Rightarrow r * d' \neq 0 \quad \forall d' \in D^*$$

infatti, se per assurdo $r * d' = 0$,

$$r * d' = 0 \Leftrightarrow (r * d')d = 0 \Leftrightarrow r * (d'd) = 0 \Leftrightarrow (r * d)d' = 0 \quad \underbrace{\Rightarrow}_{D \text{ dominio}} r * d = 0 \vee d' = 0 \quad \underbrace{\Rightarrow}_{d' \in D^*} r * d = 0$$

assurdo contro Hp. Osservando che

$$r * d' \neq 0 \quad \underbrace{\Rightarrow}_{(1)} s * d' = 0$$

concludiamo che

$$\forall d' \in D \quad s * d' = 0 \quad (2)$$

(2) Q.E.D.

$$(2) \Rightarrow s \in D_0 \Rightarrow \min D_0 \leq s \Leftrightarrow rs \leq s \Leftrightarrow r = 1$$

assurdo.

Quindi, $\text{ch}D$ e' necessariamente primo.

Supponendo adesso che D sia unitario, dimostriamo che $\text{ch}D \neq 1$. Infatti, dalla def [2.5,pg.11]

$$\text{ch}D = 1 \Rightarrow 1 \in D_0 \Rightarrow 1 * D = \{0\} \Leftrightarrow 1 * d = 0 \quad \forall d \in D \Leftrightarrow d = 0 \quad \forall d \in D \Leftrightarrow D = \{0\}$$

Ma D e' un anello unitario, e quindi, per quanto supposto in [1.1,pg.1], $\{0, 1\} \subseteq D$, $0 \neq 1$. Assurdo.

□

Proposition 2.8. *La caratteristica di un dominio unitario e' una proprieta' ereditaria: sia D un dominio unitario, e $E \subseteq D$ un suo sottodominio unitario, allora*

$$\text{ch}E = \text{ch}D$$

Proof: Poiche' $E \subseteq D$ e' un sottodominio unitario abbiamo $1_E = 1_D$. Ovvero, E e D hanno la stessa unita'. E quindi, applicando la prop [2.4,pg.11] si ha la tesi. $\square$

Proposition 2.9. *Sia K un campo, per quanto abbiamo visto in [2.7,pg.12], $\text{ch}K = 0 \vee \text{ch}K = p$. Inoltre, si ha*

$$\begin{aligned}\text{ch}K = p \text{ primo} &\Rightarrow \mathbb{Z}_p \hookrightarrow K \\ \text{ch}K = 0 &\Rightarrow \mathbb{Z} \hookrightarrow K, \quad \mathbb{Q} \hookrightarrow K\end{aligned}$$

Proof: Essendo K un campo, e' anche un anello unitario. Possiamo allora considerare γ (vedi [2.1,pg.8]):

$$\begin{aligned}\ker \gamma &\underbrace{=}_{[2.3,pg.10]} (\text{ch}K) \\ \gamma \text{ omomorfismo} &\underbrace{\Rightarrow}_{\text{thm omomorf. [AI,17.10.1,pg.86]}} \frac{Z}{\ker \gamma} \simeq \text{Im } \gamma \Leftrightarrow \frac{Z}{(\text{ch}K)} \simeq \text{Im } \gamma\end{aligned}$$

CASE: $\text{ch}K = p$

$$(\text{ch}K) = (p) \quad \frac{Z}{(\text{ch}K)} \simeq \text{Im } \gamma \Leftrightarrow \mathbb{Z}_p \simeq \text{Im } \gamma \leq K$$

CASE: $\text{ch}K = 0$

$$\ker \gamma = (\text{ch}K) = (0) \Rightarrow \gamma \text{ e' iniettiva}$$

Consideriamo un'estensione di γ :

$$\begin{aligned}\bar{\gamma} : Q(\mathbb{Z}) = \mathbb{Q} &\longrightarrow K \\ \bar{\gamma}\left(\frac{m}{n}\right) &= \gamma(m)\gamma(n)^{-1}\end{aligned}$$

Per la prop, [1.10,pg.2], $\bar{\gamma}$ e' una immersione. Allora, per il thm dell'omomorfismo, si ha:

$$\frac{\mathbb{Q}}{\ker \bar{\gamma}} = \frac{\mathbb{Q}}{(0)} \simeq \text{Im } \bar{\gamma} \leq K$$

e poiche' $\frac{\mathbb{Q}}{(0)} \simeq \mathbb{Q}$, si ha la tesi, ovvero,

$$\mathbb{Q} \simeq \text{Im } \bar{\gamma} \leq K$$

$\square$

Definition 2.10. Dato un campo K , definiamo il *sottocampo fondamentale* (o primo) di K :

$$SF(K) \stackrel{\text{def}}{=} \bigcap_{K' \preceq K} K'$$

ovvero e' il piu' piccolo sottocampo di K .

Proposition 2.11. *Sia K un campo. Inoltre, si ha*

$$\begin{aligned}\text{ch}K = 0 &\Rightarrow SF(K) \simeq \mathbb{Q} \\ \text{ch}K = p \text{ primo} &\Rightarrow SF(K) \simeq \mathbb{Z}_p\end{aligned}$$

Proof:

CASE: $\text{ch}K = p$

Sia K' un sottocampo di K , si ha $\text{ch}K' = p$, infatti,

$$k \in K' \subseteq K \Rightarrow (\text{ch}K) * k = 0 \quad \forall k \in K' \Rightarrow \text{ch}K \in K'_0 \Rightarrow K'_0 \neq \emptyset \Leftrightarrow \text{ch}K' \neq 0 \quad (1)$$

$$K' \text{ campo} \xRightarrow{[2.7, \text{pg.12}]} \text{ch}K' = 0 \vee \text{ch}K' = p \xRightarrow{(1)} \text{ch}K' = p$$

Allora, per la prop. [2.9,pg.13], si ha

$$\begin{aligned} \exists H \leq K' : H &\simeq \mathbb{Z}_p \\ \mathbb{Z}_p = (1) &\Rightarrow H = (1_{K'}) = (1_K) \end{aligned}$$

Riassumendo:

$$\forall K' \preceq K \quad (1_K) \leq K'$$

Quindi

$$SF(K) = \bigcap_{K' \preceq K} K' = (1_K) \simeq \mathbb{Z}_p$$

CASE: $\text{ch}K = 0$

Sia $K' \preceq K$, si ha $\text{ch}K' = 0$, infatti, considerando $\gamma : \mathbb{Z} \longrightarrow K$ (vedi [2.1,pg.8]), e la sua restrizione $\gamma' : \mathbb{Z} \longrightarrow K'$ (nota⁵), si ha

$$\ker \gamma = \gamma^{-1}(1_K) \xRightarrow{1_K=1_{K'}} \gamma^{-1}(1_{K'}) = \ker \gamma'$$

$$\ker \gamma' = \ker \gamma = (\text{ch}K) = (0) \Rightarrow \text{ch}K' = 0$$

Allora, per la prop. [2.9,pg.13], si ha

$$\begin{aligned} \exists D \leq K' : D &\simeq \mathbb{Z} \\ \mathbb{Z} = (1_{\mathbb{Z}}) &\Rightarrow D = (1_{K'}) = (1_K) \leq K' \end{aligned}$$

Riassumendo:

$$\forall K' \preceq K \quad (1_K) \leq K'$$

Quindi

$$\begin{aligned} SF(K) &= \bigcap_{K' \preceq K} K' \supseteq (1_K) \\ \left\{ \begin{array}{l} (1_K) \subseteq SF(K) \\ (1_K) \text{ dominio} \\ SF(K) \text{ campo} \end{array} \right. &\xRightarrow{[1.11, \text{pg.3}]} \exists H \preceq SF(K) : H \simeq Q((1_K)) \xRightarrow{(1_K) \simeq \mathbb{Z}} \mathbb{Q} \end{aligned}$$

Ma per definizione di $SF(K)$ (il piu' piccolo...), si ha:

$$H \preceq SF(K) \Rightarrow H = SF(K) \Rightarrow SF(K) \simeq \mathbb{Q}$$

□

Proposition 2.12. Sia K campo, e sia $n \in \mathbb{N}^*$, $a \in K$, allora

$$\begin{aligned} n * a &\stackrel{\text{def}}{=} \underbrace{a + a + \dots + a}_{n\text{-volte}} = \underbrace{\bar{n}a}_{\text{moltiplicazione in } K} \\ \text{dove } \bar{n} &= \begin{cases} n & SF(K) = \mathbb{Q} \Leftrightarrow \text{ch}K = 0 \\ [n]_p & SF(K) = \mathbb{Z}_p \Leftrightarrow \text{ch}K = p \\ \text{classe resto mod } p & \end{cases} \end{aligned}$$

⁵poiche' K' e' un campo, per quanto visto in [2.1,pg.8], γ' e' ancora un omomorfismo

In seguito, per abuso di notazione, scriveremo:

$$n * a = \bar{n}a = na$$

$$n = \bar{n} \in \begin{cases} \mathbb{Z} & \text{ch}K = 0 \\ \mathbb{Z}_p & \text{ch}K = p \end{cases}$$

Proof: Dimostriamo la tesi a meno di isomorfismi.

Per la [2.9,pg.13], K contiene il campo $\mathbb{Z}$ o il campo $\mathbb{Z}_p$. Sia Z il campo contenuto, Ricordando che $\mathbb{Z}$ e $\mathbb{Z}_p$ sono gruppi ciclici generati da 1,

$$\bar{n} \in Z \Rightarrow \bar{n} = \underbrace{1_Z + 1_Z + \cdots + 1_Z}_{\bar{n} \text{ volte}} \quad (1)$$

$$1_Z \in Z \subseteq K \Rightarrow 1_Z = 1_K \underset{(1)}{\Rightarrow} \bar{n} = 1_K + 1_K + \cdots + 1_K \in K$$

$$n * a \stackrel{\text{def}}{=} \underbrace{a + a + \cdots + a}_{n\text{-volte}} \underset{\text{in } K \text{ vale la distributiva}}{=} (1_K + 1_K + \cdots + 1_K)a = \bar{n}a$$

□

2.2 Estensioni

Definition 2.13. Siano K, F due campi, poniamo

$$K \text{ e' una estensione di } F \stackrel{\text{def}}{\Leftrightarrow} K \supseteq F$$

Proposition 2.14. Sia data l'estensione $K \supseteq F$, allora K e' uno spazio vettoriale il cui campo e' F .

Per indicare tale spazio vettoriale, useremo il simbolo K_F . A volte, useremo le seguenti notazioni equivalenti:

$$\dim K_F = \dim_F K = [K : F]$$

Proof: Basta ricordarsi la definizione di spazio vettoriale, campo e che $F \subseteq K \Rightarrow 1_K = 1_F$ (vedi [1.5,pg.1]). □

Proposition 2.15. Consideriamo le seguenti estensioni di F : $K \supseteq F$, $K' \supseteq F$. Si ha:

$$f : K \longrightarrow K' \text{ omomorfismo t.c. } f|_F = \text{id} \Rightarrow f : K_F \longrightarrow K'_F \text{ applicazione lineare}$$

Proof: Sia $\lambda \in F$, $a \in K$

$$\begin{cases} \lambda \in F \subseteq K, & a \in K \\ f \text{ omomorfismo} \end{cases} \Rightarrow f(\lambda a) = f(\lambda)f(a) \underset{f|_F = \text{id}}{=} \lambda f(a)$$

$$\forall \lambda \in F \forall a \in K \quad f(\lambda a) = \lambda f(a)$$

$$\forall a, b \in K \quad f(a + b) \underset{f \text{ omomorfismo}}{=} f(a) + f(b)$$

Infine, poiche' K_F, K'_F sono degli F -spazi vettoriali, si ha che f e' una applicazione lineare. □

Definition 2.16. Sia data l'estensione $K \supseteq F$,

$$K \supseteq F \text{ e' finita} \stackrel{\text{def}}{\Leftrightarrow} K_F \text{ ha dimensione finita} \Leftrightarrow \dim K_F = n \in \mathbb{N}$$

Example 2.17.

1. $\mathbb{C} \supseteq \mathbb{R}$ e' una estensione finita, infatti, una base per $\mathbb{C}_{\mathbb{R}}$ e' $\{1, i\}$, e quindi $\dim \mathbb{C}_{\mathbb{R}} = 2$.
2. $\mathbb{R} \supseteq \mathbb{Q}$ non e' una estensione finita, infatti, se per assurdo lo fosse, esisterebbe una base $\{r_1, \dots, r_n\}$ di $\mathbb{R}_{\mathbb{Q}}$, e quindi considerando il $\mathbb{Q}$ -spazio vettoriale $\mathbb{Q}^n$, si ha

$$\begin{array}{ccc} \left\{ \begin{array}{l} \dim \mathbb{R}_{\mathbb{Q}} = n = \dim \mathbb{Q}^n \\ \mathbb{R}_{\mathbb{Q}}, \mathbb{Q}^n \text{ sono } \mathbb{Q} \text{ spazi vettoriali} \end{array} \right. & \xRightarrow{\text{prop. [AL,7.6,pg.40]}} & \mathbb{R}_{\mathbb{Q}} \xrightarrow{\text{isom. vettoriale}} \mathbb{Q}^n \\ \mathbb{R}_{\mathbb{Q}} \simeq \mathbb{Q}^n \Rightarrow |\mathbb{R}| = |\mathbb{Q}^n| & \xRightarrow{\text{thm di Cantor [AI,8.5,pg.35]}} & |\mathbb{Q}| = |\mathbb{N}| \end{array}$$

e questo e' assurdo perche' $|\mathbb{R}| \neq |\mathbb{N}|$

Theorem 2.18. Siano F, K, L campi, tali che $L \supseteq K \supseteq F$, allora

$$\dim L_F < +\infty \Leftrightarrow \begin{cases} \dim K_F < +\infty \\ \dim L_K < +\infty \end{cases}$$

Se una delle due condizioni e' soddisfatta, si ha:

$$\begin{aligned} \dim L_F &= \dim L_K \dim K_F \\ BC &\text{ e' una base di } L_F, \text{ dove} \\ B &\text{ base di } K_F, C \text{ base di } L_K \\ BC &= \{bc \mid b \in B, c \in C\} \end{aligned}$$

Proof:

(1) Dim. $\Rightarrow$

$$\begin{aligned} \dim L_F = n &\Rightarrow \exists B = \{b_1, \dots, b_n\} \text{ base di } L_F \Rightarrow L_F = \mathcal{L}(B)_F \\ K \subseteq L &\Rightarrow K_F \subseteq L_F \text{ sottospazio vettoriale} \Rightarrow \dim K_F \leq \dim L_F \Rightarrow \dim K_F < +\infty \\ L_F = \mathcal{L}(B)_F &\xRightarrow{F \subseteq K} L_K = \mathcal{L}(B)_F \Rightarrow \dim L_K < +\infty \end{aligned}$$

(1) Dim. $\Leftarrow$

$$\dim K_F < +\infty \Rightarrow \exists B = \{b_1, \dots, b_m\} \text{ base di } K_F \quad (1)$$

$$\dim L_K < +\infty \Rightarrow \exists C = \{c_1, \dots, c_n\} \text{ base di } L_K \quad (2)$$

Dimostriamo che BC e' una base di L_F , dove

$$BC = \{b_i c_j \mid i = 1, \dots, m \quad j = 1, \dots, n\}$$

(1.1) Dim. che $L_F = \mathcal{L}(BC)_F$

Poiche' L contiene sia K che F che BC , e poiche' le operazioni sono chiuse in L (e' un campo), si ha subito che

$$\mathcal{L}(BC)_F \subseteq L_F$$

Dimostriamo l'inclusione inversa. Sia $a \in L$,

$$a \in L \underset{(2)}{\Rightarrow} a = k_1 c_1 + \cdots + k_n c_n = \sum_{i=1}^n k_i c_i$$

$$k_i \in K \underset{(1)}{\Rightarrow} k_i = f_{1i} b_1 + \cdots + f_{mi} b_m = \sum_{j=1}^m f_{ji} b_j$$

$$a = \sum_{i=1}^n k_i c_i = \sum_{i=1}^n \left(\sum_{j=1}^m f_{ji} b_j \right) c_i = \sum_{i=1}^n k_i c_i = \sum_{i=1}^n \sum_{j=1}^m f_{ji} b_j c_i \Rightarrow a \in \mathcal{L}(BC)$$

(1.2) Dim. che i vettori di BC sono indipendenti

Sia $o = mn$ e consideriamo la generica comb. lin. nulla dei $b_j c_i$:

$$\sum_{i=1}^n \sum_{j=1}^m x_{ji} b_j c_i = 0 \quad (*)$$

poiche' i c_i sono l.i. si ha che nella (*) i coefficienti dei c_i sono tutti nulli:

$$\sum_{j=1}^m x_{ji} b_j = 0 \quad \forall i = 1, \dots, n$$

ma poiche' i b_j sono l.i., si pure che:

$$x_{ji} = 0 \quad \forall j = 1, \dots, m \quad \forall i = 1, \dots, n$$

Così, in definitiva, i coefficienti dei $b_j c_i$ in (*) sono tutti nulli, e quindi i $b_j c_i$ sono l.i.

(1.3) $|BC| = mn = \dim K_F \dim L_K$

Poiche' i $b_j c_i$ sono l.i., sono distinti fra loro, e quindi $|BC| = mn$.

□

Corollary 2.19. Siano $K_1, \dots, K_t$, con $t \geq 3$, campi che formano la seguente catena di estensioni:

$$K_t \supseteq K_{t-1} \supseteq \dots \supseteq K_1$$

, allora

$$\dim_{K_1} K_t < +\infty \Leftrightarrow \begin{cases} \dim_{K_1} K_2 < +\infty \\ \dim_{K_2} K_3 < +\infty \\ \vdots \\ \dim_{K_{t-1}} K_t < +\infty \end{cases}$$

e inoltre, se vale una delle due condizioni, si ha

$$\dim_{K_1} K_t = \dim_{K_1} K_2 \dim_{K_2} K_3 \dots \dim_{K_{t-1}} K_t = \prod_{i=1}^{t-1} \dim_{K_i} K_{i+1}$$

Proof: Procediamo per induzione su t .

(1) $t = 3$

Basta leggere il thm [2.18,pg.16], con $L = K_3$, $K = K_2$, $F = K_1$.

(2) $t - 1 \Rightarrow t$

Per l'ipotesi induttiva abbiamo

$$\dim_{K_1} K_{t-1} < +\infty \Leftrightarrow \begin{cases} \dim_{K_1} K_2 < +\infty \\ \dim_{K_2} K_3 < +\infty \\ \vdots \\ \dim_{K_{t-2}} K_{t-1} < +\infty \end{cases} \quad (*)$$

$$\dim_{K_1} K_{t-1} = \prod_{i=1}^{t-2} \dim_{K_i} K_{i+1} \quad (**)$$

Ma allora, applicando il thm [2.18,pg.16] a K_t, K_{t-1}, K_1 , si ha

$$\dim_{K_1} K_t < +\infty \Leftrightarrow \begin{cases} \dim_{K_1} K_{t-1} < +\infty \\ \dim_{K_{t-1}} K_t < +\infty \end{cases} \xLeftrightarrow (*) \begin{cases} \dim_{K_1} K_2 < +\infty \\ \dim_{K_2} K_3 < +\infty \\ \vdots \\ \dim_{K_{t-1}} K_t < +\infty \end{cases}$$

$$\dim_{K_1} K_t = \dim_{K_1} K_{t-1} \dim_{K_{t-1}} K_t \underbrace{=}_{(**)} \prod_{i=1}^{t-1} \dim_{K_i} K_{i+1}$$

□

Definition 2.20. Sia $F \preceq K$ una estensione di campi, e siano $\alpha_1, \dots, \alpha_n \in K$. Definiamo l'estensione di F generata da $\{\alpha_1, \dots, \alpha_n\}$:

$$F(\alpha_1, \dots, \alpha_n) \stackrel{\text{def}}{=} \bigcap \{K' \preceq K \mid F \cup \{\alpha_1, \dots, \alpha_n\} \subseteq K'\}$$

ovvero, $F(\alpha_1, \dots, \alpha_n)$ e' la piu' piccola estensione di F in K che contiene $\alpha_1, \dots, \alpha_n$. Possiamo riguardare $F(\alpha_1, \dots, \alpha_n)$ come una sorta di generalizzazione del campo dei quozienti: $F(\alpha_1, \dots, \alpha_n)$ e' il piu' piccolo sottocampo che si ottiene in K "aggiungendo" in F $\alpha_1, \dots, \alpha_n$.

Proposition 2.21. Sia $F \preceq K$ una estensione di campi, e siano $\alpha_1, \dots, \alpha_n \in K$. Si ha

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in F[x_1, \dots, x_n], g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

NOTA: con $\frac{f}{g}$ stiamo indicando l'operazione fg^{-1} . Poiche' $f(\alpha_1, \dots, \alpha_n), g(\alpha_1, \dots, \alpha_n) \in K$, e K e' un campo, la notazione $\frac{f}{g}$ e' equivalente a fg^{-1} (infatti⁶)

Proof: Indichiamo con G il secondo insieme.

(1) $\text{Dim} \supseteq$

Poiche' le operazioni in $F(\alpha_1, \dots, \alpha_n)$ sono chiuse, si ha

$$\mathcal{L}(\alpha_1, \dots, \alpha_n)_F \subseteq F(\alpha_1, \dots, \alpha_n)$$

Gli elementi di $\mathcal{L}(\alpha_1, \dots, \alpha_n)_F$ sono del tipo:

$$f_1 \alpha_1 + \dots + f_n \alpha_n \quad (*)$$

⁶infatti, siano $a, b, c, d \in K$, b, d non nulli, allora

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} = (ad + bc)d^{-1}b^{-1} \\ ab^{-1} + cd^{-1} &= (ab^{-1} + cd^{-1})bdb^{-1}d^{-1} = (ad + cb)b^{-1}d^{-1} \end{aligned}$$

analogamente per la moltiplicazione.

Se moltiplichiamo $(*)$ per un α_i , otteniamo un altro elemento di $F(\alpha_1, \dots, \alpha_n)$. Quindi, tutti gli elementi del tipo:

$$f(\alpha_1, \dots, \alpha_n) \quad \text{con } f(x_1, \dots, x_n) \in F[x_1, \dots, x_n] \quad (1)$$

stanno in $F(\alpha_1, \dots, \alpha_n)$.

Poiche' $F(\alpha_1, \dots, \alpha_n)$ e' un campo, per ogni suo elemento non nullo contiene il suo inverso:

$$g(\alpha_1, \dots, \alpha_n) \neq 0 \Rightarrow \frac{1}{g(\alpha_1, \dots, \alpha_n)} \in F(\alpha_1, \dots, \alpha_n) \quad (2)$$

Ma allora, il prodotto tra un elemento del tipo (1) e uno del tipo (2) sta' sempre in $F(\alpha_1, \dots, \alpha_n)$.

Ecco quindi che $G \subseteq F(\alpha_1, \dots, \alpha_n)$.

(2) Dim $\subseteq$

(2.1) Dimostriamo che $G \preceq K$

E' chiaro che $G \subseteq K$. Usiamo la caratterizzazione dei sottoanelli: siano $a, b \in G$

$$a - b = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} - \frac{\bar{f}(\alpha_1, \dots, \alpha_n)}{\bar{g}(\alpha_1, \dots, \alpha_n)} = \frac{f(\alpha_1, \dots, \alpha_n)\bar{g}(\alpha_1, \dots, \alpha_n) + \bar{f}(\alpha_1, \dots, \alpha_n)g(\alpha_1, \dots, \alpha_n)}{\bar{f}(\alpha_1, \dots, \alpha_n)\bar{g}(\alpha_1, \dots, \alpha_n)}$$

che chiaramente appartiene ancora in G . Analogamente, $ab \in G$.

Poiche' $1_K \in G$, G e' cosi' diventato un sottoanello unitario di K .

L'inverso di ogni elemento $a \in G^*$ esiste ed e'

$$\frac{g(\alpha_1, \dots, \alpha_n)}{\bar{f}(\alpha_1, \dots, \alpha_n)}$$

Chiaramente gli elementi di G commutano ($G \subseteq K$).

Ecco che $G \preceq K$.

(2.2) Q.E.D.

E' chiaro che $F \cup \{\alpha_1, \dots, \alpha_n\} \subseteq G$. Poiche' $G \preceq K$, per definizione di $F(\alpha_1, \dots, \alpha_n)$ (il piu' piccolo...) si ha che

$$F(\alpha_1, \dots, \alpha_n) \subseteq G$$

□

Proposition 2.22. Sia $F \preceq K$ una estensione, $\alpha_1, \dots, \alpha_t \in K$, $t \geq 2$. Posto

$$F_1 = F$$

$$F_i = F(\alpha_1, \dots, \alpha_{i-1})$$

si ha

$$F_i(\alpha_i) = F_{i+1}$$

$$F_i(\alpha_i, \alpha_{i+1}, \dots, \alpha_n) = F_{n+1}$$

ovvero:

$$(F(\alpha_1, \dots, \alpha_{i-1}))(\alpha_i) = F(\alpha_1, \dots, \alpha_i)$$

$$(F(\alpha_1, \dots, \alpha_{i-1}))(\alpha_i, \alpha_{i+1}, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$$

In pratica, possiamo togliere tutte le parentesi, mettere assieme le α_i , e considerare una sola parentesi.

Proof:

(1) Dim. $F_i(\alpha_i) = F_{i+1}$

$F(\alpha_1, \dots, \alpha_i)$ e' un sottocampo di K e contiene F_i, α_i , quindi per definizione⁷

$$F_i(\alpha_i) \subseteq F(\alpha_1, \dots, \alpha_i)$$

⁷ $F_i(\alpha_i)$ e' il piu' piccolo sottocampo di K che contiene F_i, α_i

$F_i(\alpha_i)$ e' un sottocampo e contiene F_i, α_i , a sua volta F_i contiene $F, \alpha_1, \dots, \alpha_{i-1}$. Allora, per definizione,

$$F(\alpha_1, \dots, \alpha_i) \subseteq F_i(\alpha_i)$$

Quindi, $F_i(\alpha_i) = F(\alpha_1, \dots, \alpha_i)$.

(2) Dim. $F_i(\alpha_i, \alpha_{i+1}, \dots, \alpha_n) = F_{n+1}$

Poniamo

$$\begin{aligned}\bar{\alpha}_j &= \alpha_{i+j-1} \\ \bar{F}_1 &= \bar{F} = F_i \\ \bar{F}_j &= \bar{F}(\bar{\alpha}_1, \dots, \bar{\alpha}_{j-1}) \\ s_n &= 2 + n - i, \quad s'_n = n + 1\end{aligned}$$

allora la tesi equivale a

$$\begin{aligned}F_i(\alpha_i, \alpha_{i+1}, \dots, \alpha_n) &= F_{n+1} \Leftrightarrow \\ \Leftrightarrow \bar{F}(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_{1+n-i}) &= F_{n+1} \Leftrightarrow \\ \Leftrightarrow \bar{F}_{2+n-i} &= F_{n+1} \Leftrightarrow \bar{F}_{s_n} = F_{s'_n}\end{aligned}$$

Dimostriamo $\bar{F}_{s_n} = F_{s'_n}$, procedendo per induzione su n .

(2.1) Base dell'induzione: $n = i$

$$\bar{F}_{s_n} = \bar{F}_{2+n-i} = \bar{F}_2 = \bar{F}(\bar{\alpha}_1) = F_i(\alpha_i) \underbrace{=}_{1} F_{i+1} \underbrace{=}_{n=i} F_{n+1} = F_{s'_n}$$

(2.2) $n - 1 > i \Rightarrow n$

Poiche' $\bar{F} \preceq K$, $\bar{\alpha}_1, \dots, \bar{\alpha}_n \in K$, possiamo applicare ad essi il passo 1:

$$\begin{aligned}\bar{F}_{s_n} &= \bar{F}_{2+n-i} \underbrace{=}_{\text{passo 1 applicato a } \bar{F}, \bar{\alpha}_1, \dots,} \bar{F}_{1+n-i}(\bar{\alpha}_{1+n-i}) = \bar{F}_{s_{n-1}}(\bar{\alpha}_{1+n-i}) = \\ \underbrace{=}_{\text{Hp induttiva}} F_{s'_{n-1}}(\bar{\alpha}_{1+n-i}) &= F_n(\bar{\alpha}_{1+n-i}) = F_n(\alpha_n) \underbrace{=}_1 F_{n+1} = F_{s'_n}\end{aligned}$$

□

Definition 2.23.

$F \preceq K$ e' un estensione finitamente generata $\stackrel{\text{def}}{\Leftrightarrow} \exists \alpha_1, \dots, \alpha_n \in K : K = F(\alpha_1, \dots, \alpha_n)$

$F \preceq K$ e' un estensione semplice $\Leftrightarrow \exists \alpha \in K : K = F(\alpha)$

α e' un elemento primitivo di K su $F \stackrel{\text{def}}{=} K = F(\alpha)$

In genere, una estensione finitamente generata, la indicheremo con

$$F \preceq F(\alpha_1, \dots, \alpha_n)$$

intendendo l'estensione $F \preceq K$, dove

$$\alpha_1, \dots, \alpha_n \in K, \quad K = F(\alpha_1, \dots, \alpha_n)$$

Proposition 2.24.

$F \preceq K$ estensione finita $\Rightarrow F \preceq K$ e' finitamente generata

Non vale il viceversa.

Proof:

(1) Dim. $\Rightarrow$

$$F \preceq K \text{ estensione finita} \Rightarrow K_F = \mathcal{L}(b_1, \dots, b_n)_F \subseteq F(b_1, \dots, b_n)$$

Ma per definizione, $K \supseteq F(b_1, \dots, b_n)$ e quindi

$$K = F(b_1, \dots, b_n)$$

(2) Dim $\Leftarrow$

Consideriamo l'estensione

$$F \preceq F(x)$$

dove x e' una indeterminata, e quindi $F(x) = Q(F[x])$.

Per costruzione, questa estensione e' finitamente generata, ma non e' finita, perche' $\dim F(x) = +\infty$ (nota⁸)

□

Definition 2.25. Sia data l'estensione $F \preceq K$ e $\alpha \in K$.

$$\alpha \text{ e' algebrico in } F \stackrel{\text{def}}{\Leftrightarrow} \exists f(x) \in F[x], f(x) \neq 0 : f(\alpha) = 0$$

$$\alpha \text{ e' trascendente} \stackrel{\text{def}}{\Leftrightarrow} \alpha \text{ non e' algebrico}$$

$$F \preceq K \text{ e' una estensione algebrica di } F \stackrel{\text{def}}{\Leftrightarrow} \forall \alpha \in K \text{ } \alpha \text{ e' algebrico in } F$$

Usualmente, se non si specifica F , si suppone $F = \mathbb{Q}$.

Example 2.26. 1. $\sqrt{2}$ e' algebrico in $\mathbb{Q}$, infatti,

$$f(x) = x^2 - 2 \in \mathbb{Q}[x], f(\sqrt{2}) = 0$$

2. e, π sono trascendenti in $\mathbb{Q}$ (lo dimostreremo in seguito).

Da questo deduciamo che $\mathbb{Q} \preceq \mathbb{R}$ non e' una estensione algebrica di $\mathbb{R}$.

3. $\mathbb{R} \preceq \mathbb{C}$ e' una estensione algebrica. Infatti, preso $a + ib \in \mathbb{C}$,

$$f(x) = (x - a)^2 + b^2 \in \mathbb{R}[x] \quad f(a + ib) = (ib)^2 + b^2 = -b^2 + b^2 = 0$$

4. $\mathbb{Q} \preceq \mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$ e' una estensione algebrica. Infatti, preso $a + ib$

$$f(x) = (x - a)^2 + b^2 \in \mathbb{Q}[x] \quad f(a + ib) = (ib)^2 + b^2 = -b^2 + b^2 = 0$$

5. $\mathbb{Q} \preceq \mathbb{Q}(\sqrt{2})$ e' una estensione algebrica, e' finita, e ha dimensione 2.

Proof:

(1) Dimostriamo intanto che

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

Per la prop [2.21,pg.18], sappiamo che

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} \mid f(x), g(x) \in \mathbb{Q}[x], g(\sqrt{2}) \neq 0 \right\}$$

⁸Lo spazio vettoriale dei polinomi non e' finitamente generato, infatti,

$$1, x, x^2, \dots, x^n$$

sono l.i. $\forall n \in \mathbb{N}$.

Ma un polinomio in $\mathbb{Q}[x]$, calcolato in $\sqrt{2}$, e' del tipo

$$\begin{aligned} f(\sqrt{2}) &= a_0 + a_1 2^{\frac{1}{2}} + a_2 2^{\frac{2}{2}} + a_3 2^{\frac{3}{2}} + a_4 2^{\frac{4}{2}} + \dots + a_n 2^{\frac{n}{2}} = \\ &= a_0 + a_1 \sqrt{2} + a_2 2 + a_3 2\sqrt{2} + a_4 2^2 + \dots + a_n 2^{\frac{n}{2}} = \\ &= (a_0 + a_2 2 + a_4 4 + \dots) + (a_1 + 2a_3 + 4a_5 + \dots) \sqrt{2} = \alpha + \beta \sqrt{2} \end{aligned}$$

Anche l'inverso di $g(\sqrt{2})$ sara' del tipo $x + y\sqrt{2}$, infatti,

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \Leftrightarrow 2by + ax + (ay + bx)\sqrt{2} = 1 \Leftrightarrow \begin{cases} ax + 2by = 1 \\ bx + ay = 0 \end{cases} \quad (*)$$

Il determinante della matrice dei coefficienti e'

$$\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2 - 2b^2$$

Se per assurdo fosse nullo, si avrebbe:

$$a^2 - 2b^2 = 0 \Leftrightarrow a^2 = 2b^2 \Leftrightarrow a = \pm\sqrt{2}b \Rightarrow a \notin \mathbb{Q}$$

assurdo. Quindi, per Cramer, il sistema (*) ammette un'unica soluzione $(\bar{x}, \bar{y})$, ovvero, $\bar{x} + \bar{y}\sqrt{2}$ e' l'inverso di $a + b\sqrt{2}$.

Detto questo:

$$\frac{f(\sqrt{2})}{g(\sqrt{2})} = \frac{\alpha + \beta\sqrt{2}}{g(\sqrt{2})} = \frac{(\alpha + \beta\sqrt{2})g(\sqrt{2})^{-1}}{g(\sqrt{2})g(\sqrt{2})^{-1}} = (\alpha + \beta\sqrt{2})(\bar{x} + \bar{y}\sqrt{2}) = \bar{\alpha} + \bar{\beta}\sqrt{2}$$

Quindi

$$\mathbb{Q}(\sqrt{2}) = \{ \bar{\alpha} + \bar{\beta}\sqrt{2} \mid \bar{\alpha}, \bar{\beta} \in \mathbb{Q} \}$$

⟨2⟩ Dimostriamo che $\mathbb{Q}(\sqrt{2})$ e' algebrico

Sia $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, allora

$$f(x) = (x - a)^2 - 2b^2 \in \mathbb{Q}[x]$$

$$f(a + b\sqrt{2}) = (b\sqrt{2})^2 - 2b^2 = 2b^2 - 2b^2 = 0$$

⟨3⟩ Dim. che $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ e' finita, e ha dimensione 2

$(1, \sqrt{2})$ e' una base dello spazio vettoriale $\mathbb{Q}(\sqrt{2})$. Infatti, come abbiamo visto, ogni elemento di $\mathbb{Q}(\sqrt{2})$ e' del tipo $a + \sqrt{2}b$, $a, b \in \mathbb{Q}$, ovvero $\mathbb{Q}(\sqrt{2}) = \mathcal{L}(1, \sqrt{2})_{\mathbb{Q}}$. Inoltre,

$1, \sqrt{2}$ sono linearmente indipendenti, infatti, se per assurdo non lo fossero:

$$a + \sqrt{2}b = 0 \Leftrightarrow b = -\frac{a}{\sqrt{2}} \underbrace{\Rightarrow}_{a \neq 0} b \notin \mathbb{Q}$$

assurdo contro $b \in \mathbb{Q}$. Quindi $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$.

□

Proposition 2.27.

$$F \preceq K \text{ estensione finita} \Rightarrow F \preceq K \text{ e' algebrica}$$

Non vale il viceversa.

Proof: Sia $\alpha \in K$.

$$F \preceq K \text{ finita} \Rightarrow \dim K_F = n$$

$$\text{Sia } A = \{1, \alpha, \alpha^2, \dots, \alpha^n\} \subseteq K$$

$$\begin{cases} \dim K_F = n \\ |A| = n + 1 \end{cases} \Rightarrow \text{gli elementi di } A \text{ sono l.d.} \Leftrightarrow$$

$$\Leftrightarrow \exists a_0, a_1, \dots, a_n \in F, \text{ non tutti nulli: } a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$$

Allora, il polinomio cercato e':

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

infatti,

$$f(x) \in F[x], \quad f(x) \neq 0, \quad f(\alpha) = 0$$

□

Proposition 2.28. *Sia $F \preceq K$ una estensione, $\alpha \in K$. Consideriamo gli insiemi:*

$$\begin{aligned} P(\alpha, F) &\stackrel{\text{def}}{=} \{f(x) \in F[x] \mid f(\alpha) = 0, f(x) \text{ monico}\} \\ \deg P(\alpha, F) &= \{\deg f(x) \mid f(x) \in P(\alpha, F)\} \end{aligned}$$

allora

$$\alpha \text{ algebrico su } F \Rightarrow \exists! p(x) \in P(\alpha, F) : \deg p(x) = \min(\deg P(\alpha, F))$$

In altre parole, $p(x)$ e' il polinomio monico, di grado minimo, tale che $p(\alpha) = 0$. $p(x)$ viene chiamato polinomio minimo di α in F , e lo indicheremo con

$$P_{\min}(\alpha, F) \stackrel{\text{def}}{=} p(x)$$

(Nota⁹)

Infine, vale

$$\begin{cases} g(x) \in F[x] \\ g(\alpha) = 0 \end{cases} \Rightarrow p(x) \mid g(x)$$

Proof: Consideriamo il seguente omomorfismo:

$$\begin{aligned} \varphi : F[x] &\longrightarrow F(\alpha) \preceq K \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

Si ha

$$F[x] \text{ ED} \quad \underbrace{\Rightarrow}_{[\text{AI}, 21.10, \text{pg. } 105]} \quad F[x] \text{ PID } (*)$$

$$\alpha \text{ algebrico} \Rightarrow \exists f(x) \in F[x] \setminus \{0\} : f(\alpha) = 0 \Rightarrow \varphi(f(x)) = 0 \Rightarrow f(x) \in \ker \varphi \underbrace{\Rightarrow}_{f(x) \neq 0} \ker \varphi \neq \{0\}$$

$$\begin{cases} \ker \varphi \leq F[x] \\ \ker \varphi \neq (0) \end{cases} \underbrace{\Rightarrow}_{(*)} \exists \bar{p}(x) \in F[x] \setminus \{0\} : \ker f = (\bar{p}(x)) = (p(x))$$

Dove $p(x)$ e' il polinomio monico ricavato da $\bar{p}(x)$, ovvero

$$p(x) = a^{-1}\bar{p}(x)$$

dove a e' il coefficiente dell'indeterminata di grado massimo di $\bar{p}(x)$

$p(x)$ e' il polinomio minimo.

(1) Dim. $p(x)$ ha il grado minimo ed e' unico

Sia $g(x) \in F[x] \setminus \{0\} : g(\alpha) = 0$.

$$g(\alpha) = 0 \Rightarrow g(x) \in \ker \varphi = (p(x)) \Rightarrow p(x) \mid g(x) \Rightarrow \exists h(x) \in F[x] : g(x) = p(x)h(x)$$

$$\deg g(x) = \deg p(x)h(x) = \deg p(x) + \deg h(x) \quad (1)$$

Se per assurdo $\deg p(x) > \deg g(x)$, si avrebbe:

$$\deg p(x) > \deg g(x) \Rightarrow \deg p(x) + \deg h(x) > \deg g(x)$$

⁹Un polinomio e' monico quando il coefficiente dell'indeterminata di grado massimo e' 1

Assurdo.

Quindi si deve avere:

$$\deg p(x) \leq \deg g(x) \quad (2)$$

(1.1) $p(x)$ e' unico

Adesso, sia $g(x)$ anche monico e di grado minimo.

$$(2) \quad \underbrace{\deg p(x) = \deg g(x)}_{g(x) \text{ ha grado minimo}} \underbrace{\Rightarrow \deg h(x) = 0}_{(1)} \Leftrightarrow h(x) = c \in F$$

$$g(x) = cp(x)$$

Se per assurdo $c \neq 1$, allora $g(x)$ non sarebbe piu' monico, assurdo. Quindi

$$g(x) = p(x)$$

□

Definition 2.29. Sia $F \preceq K$ una estensione, $\alpha \in K$, allora

$$F[\alpha] \stackrel{\text{def}}{=} \text{Im } \varphi = \{f(\alpha) \mid f(x) \in F[x]\}$$

dove φ e' l'omomorfismo visto in [2.28,pg.23]:

$$\begin{aligned} \varphi : F[x] &\longrightarrow F(\alpha) \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

Proposition 2.30. Sia $F \preceq K$ una estensione, $\alpha \in K$, $p(x) \in F[x]$, allora

$$p(x) = P_{\min}(\alpha, F) \Leftrightarrow \begin{cases} p(x) \in F[x], & p(x) \text{ irriducibile in } F[x] \\ p(x) \text{ monico} \\ p(\alpha) = 0 \end{cases}$$

Inoltre, se una delle due condizioni e' soddisfatta, si ha:

$$\frac{F[x]}{(p(x))} \simeq F[\alpha]$$

Proof:

(1) Dim $\Rightarrow$

Basta dimostrare che $p(x)$ e' irriducibile in F .

Considerando l'omomorfismo φ visto nella dim. della prop [2.28,pg.23], si ha

$$\ker \varphi = (p(x))$$

$$\varphi : F[x] \longrightarrow F(\alpha) \text{ omomorfismo} \quad \underbrace{\Rightarrow}_{\text{thm omomorf. [AI,17.10.1,pg.86]}} \quad \frac{F[x]}{(p(x))} \simeq \text{Im } \varphi = F[\alpha] \leq F(\alpha) \quad (*)$$

$$F(\alpha) \text{ campo} \Rightarrow F(\alpha) \text{ dominio} \quad \underbrace{\Rightarrow}_{[1.9,pg.2]} \quad \text{Im } \varphi \text{ dominio} \quad \underbrace{\Rightarrow}_{(*)} \quad \frac{F[x]}{(p(x))} \text{ dominio} \quad \underbrace{\Rightarrow}_{[AI,18.3,pg.90]} \quad (p(x)) \text{ primo} \Leftrightarrow$$

$$\underbrace{\Leftrightarrow}_{[1.8,pg.2]} \quad p(x) \text{ irriducibile}$$

(2) Dim $\Leftarrow$

Basta dimostrare che $p(x)$ ha grado minimo.

Sia $g(x) = P_{\min}(\alpha, F)$, allora

$$\ker \varphi = (g(x))$$

$$p(\alpha) = 0 \Rightarrow p(x) \in \ker \varphi = (g(x)) \Leftrightarrow p(x) = h(x)g(x)$$

$$\begin{cases} p(x) = h(x)g(x) \\ p(x) \text{ irriducibile} \end{cases} \Rightarrow h(x) \text{ invertibile} \vee g(x) \text{ invertibile} \Leftrightarrow$$

$$\Leftrightarrow \deg h(x) = 0 \vee \deg g(x) = 0 \xRightarrow{\deg g(x) > 0} \deg h(x) = 0 \Leftrightarrow h(x) = c \in F \Rightarrow p(x) = cg(x)$$

$$\begin{cases} p(x) = cg(x) \\ p(x) \text{ monico} \end{cases} \Rightarrow c = 1 \Rightarrow p(x) = g(x)$$

Quindi $p(x)$ e' proprio il polinomio minimo di α .

□

Example 2.31. Sia $\alpha \in F$, F campo, allora, il polinomio minimo di α in F e'

$$P_{\min}(\alpha, F) = x - \alpha$$

infatti,

$$x - \alpha \in F[x], \text{ e' monico e ha grado minimo}$$

Example 2.32. Sia $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $a + \sqrt{2}b \in K$, $b \neq 0$. Come abbiamo visto in [5,pg.21],

$$f(x) = (x - a)^2 - 2b^2 \in \mathbb{Q}[x]$$

e' un polinomio in $\mathbb{Q}[x]$ t.c. $f(\alpha) = 0$. E' monico. Inoltre, e' irriducibile in $\mathbb{Q}$: se per assurdo fosse riducibile in $\mathbb{Q}$, essendo di secondo grado, sarebbe diviso da un polinomio di primo grado in $\mathbb{Q}$:

$$(x - \beta) \mid f(x), \quad \beta \in \mathbb{Q} \Rightarrow f(\beta) = 0, \quad \beta \in \mathbb{Q}$$

ma le uniche radici di $f(x)$ sono $a + \sqrt{2}b$, $a - \sqrt{2}b$, che certamente non sono in $\mathbb{Q}$. Quindi, $f(x)$ e' irriducibile in $\mathbb{Q}$. Allora, per la prop. [2.30,pg.24], $f(x)$ e' il polinomio minimo di $a + \sqrt{2}b$ in $\mathbb{Q}$.

Proposition 2.33. Sia $F \preceq K$ una estensione, con $\alpha \in K$, allora

$$\alpha \text{ trascendente su } F \Rightarrow F(\alpha) \simeq F(x), \text{ con } x \text{ indeterminata}$$

Proof: Consideriamo la seguente applicazione:

$$\begin{aligned} \varphi : F(x) &\longrightarrow F(\alpha) \\ \frac{f(x)}{g(x)} &\mapsto \frac{f(\alpha)}{g(\alpha)} \end{aligned}$$

(1) φ e' ben posta

$$\alpha \text{ trascendente su } F \Rightarrow \forall g(x) \in F[x] \quad g(\alpha) \neq 0 \Rightarrow \exists \frac{1}{g(\alpha)} \Rightarrow \frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$$

(2) φ e' un omomorfismo

E' immediato.

(3) φ e' surriettivo

Per la prop. [2.21,pg.18], abbiamo che

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

e quindi, preso un

$$\frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$$

come controimmagine, basta considerare

$$\frac{f(x)}{g(x)}$$

(4) φ e' iniettiva

Considerando che

$$\frac{g(x)}{g(x)} \mapsto 1 \Rightarrow \text{Im } \varphi \neq \{0\}$$

basta applicare la prop. [AI,18.2,pg.90].

□

Proposition 2.34. Sia $F \preceq K$ una estensione e $\alpha \in K$, si ha

$$\alpha \text{ trascendente su } F \Rightarrow F[x] \simeq F[\alpha]$$

Proof:

(1) Dim. $\Rightarrow$

Consideriamo l'omomorfismo surriettivo visto in [2.30,pg.24]:

$$\varphi : F[x] \longrightarrow F[\alpha]$$

$$f(x) \mapsto f(\alpha)$$

Si ha

$$\ker \varphi = [f(x) \in F[x] \mid f(\alpha) = 0] \underbrace{=}_{\alpha \text{ trascendente su } F} \{0\} \Rightarrow \varphi \text{ e' iniettiva}$$

Allora, φ e' un isomorfismo:

$$F[x] \simeq F[\alpha]$$

□

Lemma 2.35. Sia $F \preceq K$ una estensione, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$. Si ha

$$\begin{cases} \alpha \text{ algebrico in } F \\ \deg p(x) = n \end{cases} \Rightarrow \forall f(\alpha) \in F[\alpha] \exists (a_0, a_1, \dots, a_n) \in F^n : f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$$

Proof:

(1) Dimostriamo l'esistenza

Sia $f(x) \in F[x]$. Poiche' $F[x]$ e' un ED, possiamo dividere $f(x)$ per $p(x)$:

$$f(x) = p(x)q(x) + r(x), \quad \deg r(x) < \deg p(x) \vee r = 0 \Rightarrow r(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \vee r = 0 \quad (*)$$

$$f(\alpha) = \underbrace{p(\alpha)}_{=0} q(\alpha) + r(\alpha) = r(\alpha)$$

$$f(\alpha) = r(\alpha)$$

in entrambi i casi, per la (*) si ha:

$$\exists (a_0, a_1, \dots, a_{n-1}) \in F^n : f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$$

(2) Dimostriamo l'unicita'

Considerando la solita φ vista in [2.28,pg.23], abbiamo

$$f(\alpha) = \underbrace{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}}_{h(\alpha)} = \underbrace{b_0 + b_1\alpha + b_2\alpha^2 + \dots + b_{n-1}\alpha^{n-1}}_{g(\alpha)} \Rightarrow$$

$$\Rightarrow \varphi(h(x)) = \varphi(g(x)) \Leftrightarrow \varphi(h(x)) - \varphi(g(x)) = 0 \Leftrightarrow \varphi(h(x) - g(x)) = 0 \Leftrightarrow h(x) - g(x) \in \ker \varphi = (p(x)) \Rightarrow$$

$$\Rightarrow p(x) \mid h(x) - g(x) \Rightarrow \deg p(x) \leq \deg(h(x) - g(x)) \vee h(x) - g(x) \equiv 0 \quad (*)$$

$$\deg h(x) \leq n-1, \deg g(x) \leq n-1 \Rightarrow \deg(h(x) - g(x)) \leq n-1 < n = \deg p(x) \underset{(*)}{\Rightarrow} h(x) - g(x) \equiv 0 \Leftrightarrow$$

$$h(x) \equiv g(x) \Leftrightarrow (a_0, a_1, \dots, a_n) = (b_0, b_1, \dots, b_n)$$

□

Theorem 2.36. Sia $F \preceq K$ una estensione, $\alpha \in K$, allora

$$\alpha \text{ e' algebrico su } F \Leftrightarrow F(\alpha) = F[\alpha]$$

Proof:

(1) Dim. $\Rightarrow$

$$\text{Sia } p(x) = P_{\min}(\alpha, F),$$

$$p(x) \text{ pol. minimo} \underset{[2.30, \text{pg.24}]}{\Rightarrow} p(x) \text{ irriducibile} \underset{[1.8, \text{pg.2}]}{\Leftrightarrow} (p(x)) \text{ massimale} \underset{[\text{AI.18.6, pg.92}]}{\Leftrightarrow} \frac{F[x]}{(p(x))} \text{ campo } (*)$$

$$\frac{F[x]}{(p(x))} \underset{[2.30, \text{pg.24}]}{\simeq} F[\alpha] \underset{(*)}{\Rightarrow} F[\alpha] \text{ campo } (**)$$

$$F[\alpha] \leq F(\alpha) \leq K \underset{(**)}{\Rightarrow} F[\alpha] \preceq K$$

Per definizione¹⁰ di $F(\alpha)$, si ha

$$\begin{cases} F \cup \{\alpha\} \subseteq F[\alpha] \\ F[\alpha] \text{ sottocampo} \Rightarrow F(\alpha) \subseteq F[\alpha] \end{cases}$$

Ma d'altronde, proprio per definizione di $F[\alpha]$, si ha $F[\alpha] \subseteq F(\alpha)$, quindi $F(\alpha) = F[\alpha]$.

(1) Dim. $\Leftarrow$

Se $\alpha = 0$, allora e' chiaro che α e' algebrico su F . Supponiamo che $\alpha \neq 0$.

$$\frac{1}{\alpha} \in F(\alpha) = F[\alpha] \Rightarrow \frac{1}{\alpha} = a_0 + a_1\alpha + \dots + a_t\alpha^t \Leftrightarrow 0 = -1 + a_0\alpha + a_1\alpha^2 + \dots + a_t\alpha^{t+1}$$

Quindi, un polinomio in $F[x]$, non nullo, che ha come radice α , e'

$$f(x) = -1 + a_0x + a_1x^2 + \dots + a_tx^{t+1}$$

□

Corollary 2.37. Sia $F \preceq K$, $\alpha \in K$, $p(x) \in F[x]$

$$p(x) = P_{\min}(\alpha, F) \Rightarrow \frac{F[x]}{(p(x))} \simeq F[\alpha] = F(\alpha)$$

Proof: Osservando che

$$p(x) = P_{\min}(\alpha, F) \Rightarrow p(x) \in F[x], p(\alpha) = 0 \Rightarrow \alpha \text{ algebrico in } F$$

basta applicare la [2.30,pg.24] e la [2.36,pg.27].

□

¹⁰ $F(\alpha)$ e' il piu' piccolo sottocampo di K contenente F, α

Corollary 2.38. Sia $F \preceq K$ una estensione, $p(x) \in F[x]$, $\alpha, \beta \in K$, si ha

$$\begin{cases} p(x) \text{ irriducibile in } F \\ p(\alpha) = p(\beta) = 0 \end{cases} \Rightarrow F(\alpha) \simeq F(\beta)$$

Inoltre,

$$\begin{aligned} \varphi|_F &= \text{id} \\ \varphi(\alpha) &= \beta \end{aligned}$$

dove $\varphi : F(\alpha) \longrightarrow F(\beta)$ e' l'isomorfismo della tesi e $\varphi|_F$ e' la restrizione di φ a F . In pratica φ sostituisce α con β .

Proof: Sia $p(x) = a\bar{p}(x)$, con $\bar{p}(x) \in F[x]$ monico. Si ha
 $p(\alpha) = p(\beta) = 0 \Rightarrow \bar{p}(\alpha) = \bar{p}(\beta) = 0$ (1)

$p(x)$ irriducibile in $F \Rightarrow \bar{p}(x)$ irriducibile in F (2)

$$\begin{aligned} \left\{ \begin{array}{l} (1), (2) \\ \bar{p}(x) \text{ monico} \end{array} \right. & \xRightarrow{\substack{[2.30, \text{pg.24}]} } \bar{p}(x) = P_{\min}(\alpha, F) = P_{\min}(\beta, F) \xRightarrow{\substack{[2.30, \text{pg.24}]} } F[\alpha] \simeq \frac{F[x]}{(p(x))} \simeq F[\beta] \Rightarrow F[\alpha] \simeq F[\beta] \quad (3) \\ \alpha, \beta \text{ algebrici su } F & \xRightarrow{\substack{[2.36, \text{pg.27}]} } F[\alpha] = F(\alpha), \quad F[\beta] = F(\beta) \xRightarrow{\substack{(3)}} F(\alpha) \simeq F(\beta) \end{aligned}$$

Infine, esaminando gli isorfismi usati abbiamo:

$$\begin{aligned} \alpha \in F[\alpha] &\mapsto x + (p(x)) \in \frac{F[x]}{(p(x))} \mapsto \beta \in F[\beta] \\ &\Rightarrow \varphi(\alpha) = \beta \\ c \in F \subseteq F[\alpha] &\mapsto c + (p(x)) \in \frac{F[x]}{(p(x))} \mapsto c \in F[\beta] \\ &\Rightarrow \varphi|_F = \text{id} \end{aligned}$$

□

Proposition 2.39. Sia F un campo, $\alpha \in K$, allora

$$F(\alpha) \simeq Q(F[\alpha])$$

ovvero l'estensione di F generata da α , e' il campo dei quozienti di $F[\alpha]$.

Proof: Sia

$$\begin{aligned} D &= F[\alpha] \\ K &= F(\alpha) \end{aligned}$$

(1) D e' un dominio

CASE: α algebrica su F

Per la [2.36,pg.27] si ha:

$$F(\alpha) = F[\alpha]$$

$F(\alpha)$ e' per definizione un campo $\Rightarrow F(\alpha)$ dominio $\Rightarrow F[\alpha]$ dominio

CASE: α trascendente

Per la prop [2.34,pg.26] si ha $F[x] \simeq F[\alpha]$, quindi

$$F[x] \text{ dominio} \Rightarrow F[\alpha] \text{ dominio}$$

Quindi, D e' un dominio, K e' un campo. Possiamo allora applicare la prop [1.10,pg.2]. Consideriamo la seguente applicazione:

$$f : Q(D) \longrightarrow K$$

$$\frac{h(\alpha)}{g(\alpha)} \mapsto h(\alpha)g(\alpha)^{-1}$$

Applicando la prop. [1.10,pg.2], con $\varphi = \text{id}$, si ha che f e' una immersione.

Per la prop [2.21,pg.18], f e' surriettiva.

Quindi $Q(D) \simeq K$. □

Proposition 2.40. *Sia $F \preceq K$ una estensione, $\alpha \in K$ e sia $p(x) = P_{\min}(\alpha, F)$, con $\dim p(x) = n$, allora*

$$\alpha \text{ algebrico in } F \Leftrightarrow F \preceq F(\alpha) \text{ estensione finita}$$

O piu' in dettaglio:

$$\alpha \text{ algebrico in } F \Leftrightarrow \dim_F F(\alpha) = n, \text{ una base di } F(\alpha) \text{ e' } \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

Proof:

(1) Dim. $\Rightarrow$

$$\alpha \text{ algebrico} \underbrace{\Rightarrow}_{[2.36, \text{pg.27}]} F(\alpha) = F[\alpha]$$

a questo punto, basta applicare la proposizione [2.35,pg.26], e si ha che una base di $F[\alpha]$ su F e' proprio

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

(1) Dim. $\Leftarrow$

$$\dim_F F(\alpha) = n \Rightarrow F \preceq F(\alpha) \text{ estensione finita} \underbrace{\Rightarrow}_{[2.27, \text{pg.22}]} F \preceq F(\alpha) \text{ estensione algebrica} \Rightarrow \alpha \text{ algebrico su } F$$

□

Proposition 2.41. *Sia $F \preceq K$ una estensione, $\alpha \in K$, allora*

$$\alpha \text{ algebrico in } F \Rightarrow \dim_F F(\alpha) = \min \{t \mid \alpha^t \in \mathcal{L}(1, \alpha, \dots, \alpha^{t-1})_F\}$$

In altre parole, per trovare la dimensione di $F(\alpha)_F$, si puo' procedere come segue:

1. si considera α^t
2. si parte da $t = 1$
3. se α^t e' combinazione lineare dei precedenti $1, \alpha, \alpha^2, \dots, \alpha_{t-1}$, ci fermiamo. t e' la dimensione cercata.
4. altrimenti si incrementa t di uno, e si ricomincia dal passo 3

Nota: una volta nota la dimensione di $F(\alpha)_F$, grazie alla [2.40,pg.29], si puo' ricavare la base di $F(\alpha)_F$.

Proof:

$$\alpha \text{ algebrico in } F \underbrace{\Rightarrow}_{[2.28, \text{pg.23}]} \exists P_{\min}(\alpha, F)$$

Sia $n = \deg P_{\min}(\alpha, F)$. Per la prop. [2.40,pg.29],

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\} \text{ e' una base di } F(\alpha)_F \quad (1)$$

$$\Rightarrow \dim_F F(\alpha) = n$$

$$\Rightarrow F(\alpha)_F = \mathcal{L}(1, \alpha, \alpha^2, \dots, \alpha^{n-1})_F \quad (1.1)$$

Poiche' $F(\alpha)_F$ e' uno spazio vettoriale finitamente generato, l'insieme $T = \{t \mid \alpha^t \in \mathcal{L}(1, \alpha, \dots, \alpha^{t-1})_F\}$ e' sicuramente non vuoto. Sia allora $m = \min T$.

Bisogna dimostrare che $m = n$. Si ha

$$\alpha^n \in F(\alpha)_F \underset{(1.1)}{=} \mathcal{L}(1, \alpha, \alpha^2, \dots, \alpha^{n-1})_F \Rightarrow n \in T \Rightarrow m \leq n$$

(1) Supponiamo per assurdo che $m < n$

$$m < n \Leftrightarrow m \leq n-1 \Rightarrow \{1, \alpha, \dots, \alpha^m\} \subseteq \{1, \alpha, \dots, \alpha^{n-1}\} \underset{(1)}{\Rightarrow} \{1, \alpha, \dots, \alpha^m\} \text{ sono l.i.}$$

$$m = \min T \Rightarrow m \in T \Rightarrow \alpha^m \in \mathcal{L}(1, \alpha, \dots, \alpha^{m-1}) \Rightarrow \{1, \alpha, \dots, \alpha^m\} \text{ non sono l.i.}$$

Assurdo.

□

Proposition 2.42. Sia $F \subseteq K$ una estensione, e siano $\alpha_1, \dots, \alpha_t \in K$, allora

$$\alpha_i \text{ algebrico in } F \quad \forall i = 1, \dots, t \Rightarrow \dim_F F(\alpha_1, \dots, \alpha_t) \leq n_1 n_2 \dots n_t$$

dove

$$n_i = \deg p_i(x), \quad p_i(x) = P_{\min}(\alpha_i, F)$$

Proof:

(1) Posto

$$F_1 = F$$

$$F_i = F(\alpha_1, \dots, \alpha_{i-1})$$

si ha

$$F_i(\alpha_i) = F_{i+1}$$

Basta usare la prop [2.22,pg.19].

(2) Dim. che $n'_i \leq n_i$, dove $n'_i = \deg p'_i(x)$, con $p'_i(x) = P_{\min}(\alpha_i, F_i)$

Si ha

$$p_i(x) \in F[x] \underset{F \subseteq F_i}{\subseteq} F_i[x]$$

$$p'_i(x) = P_{\min}(\alpha_i, F_i) \Rightarrow \deg p'_i(x) = \min(\deg P(\alpha_i, F_i)) \quad (*)$$

$$\begin{cases} p_i(x) \in F_i[x] \\ p_i(\alpha_i) = 0 \\ p_i(x) \text{ e' monico} \end{cases} \Rightarrow p_i(x) \in P(\alpha_i, F_i) \underset{(*)}{\Rightarrow} \deg p'_i(x) \leq \deg p_i(x)$$

A priori non possiamo essere sicuri sull'uguaglianza. Mostriamo un esempio:

$$\alpha_1 = \sqrt{2}, \quad F = \mathbb{Q}, \quad F_1 = \mathbb{Q}(\sqrt{2})$$

$$p_1(x) = P_{\min}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$$

infatti, $x^4 - 2$ e' monico e irriducibile in $\mathbb{Q}$. La sua fattorizzazione completa e':

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$$

$$p'_1(x) = P_{\min}(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) = x^2 - \sqrt{2}$$

E abbiamo

$$\deg p'_1(x) = 2 < \deg p_1(x) = 4$$

$$\langle 3 \rangle \dim_{F_i} F_{i+1} \leq n_i$$

$$\begin{aligned} \alpha_i \text{ algebrico in } F &\xRightarrow{F \subseteq F_i} \alpha_i \text{ algebrico in } F_i \xRightarrow{[2.40, \text{pg.29}]} \dim_{F_i} F_i(\alpha_i) = \deg p'_i(x) = n'_i \underbrace{\leq}_2 n_i \\ \dim_{F_i} F_i(\alpha_i) &\leq n_i \underbrace{\Leftrightarrow}_1 \dim_{F_i} F_{i+1} \leq n_i \end{aligned}$$

$\langle 4 \rangle$ Q.E.D.

Consideriamo la catena di estensioni:

$$F_1 \preceq F_2 \preceq \dots \preceq F_{t+1}$$

che per il passo 1 equivale a

$$F \preceq F(\alpha_1) \preceq F(\alpha_1, \alpha_2) \preceq \dots \preceq F(\alpha_1, \dots, \alpha_t)$$

Per il passo 3, si ha

$$\dim_{F_1} F_2 \leq n_1$$

$$\dim_{F_2} F_3 \leq n_2$$

$\vdots$

$$\dim_{F_t} F_{t+1} \leq n_t$$

$$\Rightarrow \dim_{F_1} F_2 \dim_{F_2} F_3 \dots \dim_{F_t} F_{t+1} \leq n_1 n_2 \dots n_t \xLeftrightarrow{[2.19, \text{pg.17}]} \dim_{F_1} F_{t+1} \leq n_1 n_2 \dots n_t \Leftrightarrow$$

$$\underbrace{\Leftrightarrow}_1 \dim_F F(\alpha_1, \dots, \alpha_t) \leq n_1 \dots n_t$$

□

Corollary 2.43. *Nelle ipotesi della prop [2.42,pg.30], si ha*

$$\alpha_i \text{ algebrico in } F \ \forall i = 1, \dots, t \Rightarrow F \preceq F(\alpha_1, \dots, \alpha_t) \text{ estensione algebrica}$$

Proof: Immediata conseguenza della prop [2.42,pg.30] e della [2.27,pg.22] □

Theorem 2.44. *Sia $F \preceq K$ una estensione, allora*

$$F \preceq K \text{ finita} \Leftrightarrow F \preceq K \text{ algebrica e finitamente generata}$$

Proof:

$\langle 1 \rangle$ Dim. $\Rightarrow$

Diretta applicazione delle proposizioni [2.27,pg.22], [2.24,pg.20].

$\langle 1 \rangle$ Dim. $\Leftarrow$

$$F \preceq K \text{ f.g.} \Rightarrow \exists \alpha_1, \dots, \alpha_t \in K : K = F(\alpha_1, \dots, \alpha_t) \quad (*)$$

$$F \preceq K \text{ algebrica} \Rightarrow \alpha_i \text{ algebrico in } F \ \forall i = 1, \dots, t \xRightarrow{[2.42, \text{pg.30}]} F \preceq F(\alpha_1, \dots, \alpha_t) \text{ e' finita} \xLeftrightarrow{(*)} F \preceq K \text{ e' finita}$$

□

Corollary 2.45. *Siano $K_1, \dots, K_t$, con $t \geq 3$, campi che formano la seguente catena di estensioni:*

$$K_t \succeq K_{t-1} \succeq \dots \succeq K_1$$

allora

$$K_t \succeq K_1 \text{ algebrica} \Leftrightarrow \begin{cases} K_1 \preceq K_2 \text{ algebrica} \\ K_2 \preceq K_3 \text{ algebrica} \\ \vdots \\ K_{t-1} \preceq K_t \text{ algebrica} \end{cases}$$

Proof: Procediamo per induzione su t .

(1) $t = 3$

(1.1) Dim. $\Rightarrow$

Sia $\alpha \in K_2$, si ha

$$\alpha \in K_2 \preceq K_3 \underbrace{\Rightarrow}_{K_1 \preceq K_3 \text{ algebrica}} \exists f \in K_1[x] \setminus \{0\} : f(\alpha) = 0 \\ \Rightarrow K_1 \preceq K_2 \text{ algebrica}$$

e quindi $K_1 \preceq K_2$ e' algebrica.

Sia $\alpha \in K_3$, come prima si vede che $K_1 \preceq K_3$ e' algebrica, ma

$$K_1 \preceq K_3 \text{ algebrica} \underbrace{\Rightarrow}_{K_1 \subseteq K_2} K_2 \preceq K_3 \text{ algebrica}$$

(1.1) Dim. $\Leftarrow$

Sia $\alpha \in K_3$,

$$K_2 \preceq K_3 \text{ algebrica} \Rightarrow \exists f \in K_2[x] \setminus \{0\} : f(\alpha) = 0 \Leftrightarrow \exists a_0, a_1, \dots, a_n \in K_2 : a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

$$\begin{cases} K_1 \leq K_2 \text{ algebrica} \\ a_0, a_1, \dots, a_n \in K_2 \end{cases} \Rightarrow a_i \text{ algebrico in } K_1 \quad \forall i = 0, 1, \dots, n \quad \underbrace{\Rightarrow}_{[2.42, \text{pg. } 30]} K_1 \preceq K_1(a_0, a_1, \dots, a_n) \text{ finita} \quad (1)$$

Sia $\overline{K}_1 = K_1(a_0, \dots, a_n)$,

$$[a_0, \dots, a_n] \in \overline{K}_1 \Rightarrow f(x) = a_0 + a_1x + \dots + a_nx^n \in \overline{K}_1[x] \quad (2)$$

Consideriamo l'estensione

$$\overline{K}_1 \preceq \overline{K}_1(\alpha) \underbrace{=}_{[2.22, \text{pg. } 19]} K_1(a_0, \dots, a_n, \alpha)$$

α e' algebrico in $\overline{K}_1$, infatti, (2.1)

$$f \neq 0, f(\alpha) = 0, f(x) \underbrace{\in}_{(2)} \overline{K}_1[x]$$

$$(2.1) \quad \underbrace{\Leftrightarrow}_{[2.40, \text{pg. } 29]} \overline{K}_1 \preceq \overline{K}_1(\alpha) \text{ e' finita} \quad (3)$$

In conclusione:

$$\begin{cases} K_1 \preceq \overline{K}_1 \preceq \overline{K}_1(\alpha) \\ (1), (3) \end{cases} \underbrace{\Rightarrow}_{[2.18, \text{pg. } 16]} K_1 \preceq \overline{K}_1(\alpha) \text{ e' finita} \underbrace{\Rightarrow}_{[2.44, \text{pg. } 31]} K_1 \preceq \overline{K}_1(\alpha) \text{ e' algebrica} \Rightarrow \alpha \text{ e' algebrico in } K_1$$

Abbiamo cosi' dimostrato, che preso un qualunque $\alpha \in K_3$, α e' algebrico in K_1 , ovvero

$$K_1 \preceq K_3 \text{ e' algebrica}$$

(2) $t - 1 \Rightarrow t$

$$K_1 \preceq K_{t-1} \preceq K_t \text{ algebrica} \underbrace{\Leftrightarrow}_1 \left\{ \begin{array}{l} K_1 \preceq K_{t-1} \text{ algebrica} \\ K_{t-1} \preceq K_t \text{ algebrica} \end{array} \right. \underbrace{\Leftrightarrow}_{\text{Hp induttiva}} \left\{ \begin{array}{l} K_1 \preceq K_2 \text{ algebrica} \\ K_2 \preceq K_3 \text{ algebrica} \\ \vdots \\ K_{t-1} \preceq K_t \text{ algebrica} \end{array} \right. \quad \square$$

Corollary 2.46. *Sia $F \preceq K$ estensione di campi, allora il seguente insieme:*

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

e' un campo.

Proof: Per la [1.6,pg.1], basta provare che

$$\forall \alpha \in \overline{F} \left\{ \begin{array}{l} 1. \alpha - \beta \in \overline{F} \quad \forall \beta \in \overline{F} \\ 2. \alpha\beta^{-1} \in \overline{F} \quad \forall \beta \in \overline{F} \setminus \{0\} \end{array} \right.$$

Siano $\alpha, \beta \in \overline{F}$, allora

$$\alpha, \beta \in \overline{F} \Rightarrow \alpha, \beta \text{ algebrici in } F \xRightarrow{[2.42, \text{pg.30}]} F \preceq F(\alpha, \beta) \text{ finita} \xRightarrow{[2.44, \text{pg.31}]} F \preceq F(\alpha, \beta) \text{ algebrica} \quad (1)$$

$$F(\alpha, \beta) \text{ campo} \Rightarrow \alpha - \beta, \alpha\beta^{-1} \in F(\alpha, \beta) \xRightarrow{(1)} \alpha - \beta, \alpha\beta^{-1} \text{ algebrici in } F \Rightarrow \alpha - \beta, \alpha\beta^{-1} \in \overline{F} \quad \square$$

Proposition 2.47. *Sia*

1. $F \preceq K$
2. $\alpha, \beta \in K$
3. $f(x) = P_{\min}(\alpha, F), \quad g(x) = P_{\min}(\beta, F)$

si ha

$$f(x) \text{ e' irriducibile in } F(\beta) \Leftrightarrow g(x) \text{ e' irriducibile in } F(\alpha)$$

Proof:

(1) Dim $\Rightarrow$

Sia $\deg f(x) = n$, $\deg g(x) = m$,

$$f(x) = P_{\min}(\alpha, F) \xRightarrow{[2.30, \text{pg.24}]} \begin{cases} f(\alpha) = 0 \\ f(x) \text{ monico} \\ f(x) \in F[x] \subseteq F(\beta)[x] \end{cases} \quad (1)$$

$$\begin{cases} f(x) \text{ irriducibile in } F(\beta) \\ (1) \end{cases} \xRightarrow{[2.30, \text{pg.24}]} f(x) = P_{\min}(\alpha, F(\beta)) \xRightarrow{[2.40, \text{pg.29}]} [F(\beta)(\alpha) : F(\beta)] = \deg f(x) = n \Leftrightarrow$$

$$\xLeftrightarrow{[2.22, \text{pg.19}]} [F(\alpha, \beta) : F(\beta)] = n$$

$$g(x) = P_{\min}(\beta, F) \xRightarrow{[2.40, \text{pg.29}]} [F(\beta) : F] = m$$

$$\begin{cases} [F(\alpha, \beta) : F(\beta)] = n \\ [F(\beta) : F] = m \end{cases} \xRightarrow{[2.18, \text{pg.16}]} [F(\alpha, \beta) : F] = mn \quad (2)$$

$$f(x) = P_{\min}(\alpha, F) \Rightarrow [F(\alpha) : F] = n$$

$$f(x) \text{ monico} \Rightarrow n > 0$$

$$[F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] \xRightarrow{[2.18, \text{pg.16}]} [F(\alpha, \beta) : F] \xLeftrightarrow{(2)} [F(\alpha, \beta) : F(\alpha)]n = mn \xLeftrightarrow{n \neq 0} [F(\alpha, \beta) : F(\alpha)] = m \Leftrightarrow$$

$$\Leftrightarrow [F(\alpha)(\beta) : F(\alpha)] = m \xRightarrow{[2.40, \text{pg.29}]} \deg P_{\min}(\beta, F(\alpha)) = m \quad (3)$$

$$\begin{cases} g(\beta) = 0 \\ g(x) \in F[x] \subseteq F(\alpha)[x] \\ g(x) \text{ monico} \\ \deg g(x) = m = \deg P_{\min}(\beta, F(\alpha)) \end{cases} \xRightarrow{\text{unicita' del polin. minimo [2.28, pg.23]}} g(x) = P_{\min}(\beta, F(\alpha)) \Rightarrow$$

$$\xRightarrow{[2.30, \text{pg.24}]} g(x) \text{ e' irriducibile in } F(\alpha)$$

(2) Dim $\Leftarrow$

Per il viceversa basta riapplicare la $\Rightarrow$, scambiando α con β e f con g .

□

2.3 Campi di spezzamento

Proposition 2.48. *Sia F un campo, $f(x) \in F[x]$, $\deg f(x) = n$. Si ha*

$$f(x) \text{ irriducibile in } F[x], \quad n \geq 1 \Rightarrow \exists F', K \text{ campi: } F \simeq F' \preceq K, \dim_{F'} K = n, \exists \alpha \in K : f'(\alpha) = 0$$

dove $f'(x)$ e' l'immagine di $f(x)$ tramite l'indotto dell'isomorfismo $F \simeq F'$.

In pratica, a meno di isomorfismi, riusciamo a trovare un campo K che contiene delle radici di $f(x)$.

Nota: a volte, scriveremo direttamente $F \subseteq K$, $f(\alpha) = 0$. Cio' che verra' dimostrato usando questa scrittura sara' effettivamente valido fino a quando non faremo esplicitamente ricorso alle proprieta' non algebriche degli elementi di K .

Proof: Sia $I = (f(x))$, si ha

$$f(x) \text{ irriducibile} \quad \underbrace{\Leftrightarrow}_{F[x] \text{ ED, [1.8,pg.2]}} \quad (f(x)) \text{ massimale} \quad \underbrace{\Leftrightarrow}_{[AI,18.6,pg.92]} \quad \frac{F[x]}{I} \text{ campo}$$

Consideriamo il seguente omomorfismo tra campi:

$$\varphi : F \longrightarrow \frac{F[x]}{I}$$

$$a \mapsto a + I$$

(e' immediato verificare che e' un omomorfismo).

$\text{Im } \varphi \neq \{0\}$, infatti, se per assurdo $\forall a \in F : a \in I$,

$$a \in I = (f(x)) \Rightarrow a = h(x)f(x) \Rightarrow \underbrace{\deg a = \deg h(x)f(x)}_{=0} = \deg h(x) + \deg f(x) \Leftrightarrow 0 = \deg h(x) + \deg f(x)$$

assurdo perche' $\deg f(x) \geq 1$.

$$F \text{ campo, } \text{Im } f \neq \{0\} \quad \underbrace{\Rightarrow}_{[AI,18.2,pg.90]} \quad \varphi \text{ iniettiva}$$

Sia $L = \frac{F[x]}{I}$.

(1) $\text{Dim } \exists \alpha \in L : f'(\alpha) = 0$

Adesso troviamo α . Consideriamo l'omomorfismo indotto da φ (vedi [1.13,pg.3]):

$$\tilde{\varphi} : F[t] \longrightarrow L[t]$$

$$\varphi \text{ iniettiva} \quad \underbrace{\Rightarrow}_{[1.13,pg.3]} \quad \tilde{\varphi} \text{ iniettiva}$$

$$\text{Sia } f'(t) = \tilde{\varphi}(f(t))$$

$\alpha = x + I \in L = \frac{F[x]}{I}$ e' la radice cercata, infatti,

$$f(t) = \sum_{i=0}^n a_i t^i \xrightarrow{\tilde{\varphi}} f'(t) = \sum_{i=0}^n \varphi(a_i) t^i = \sum_{i=0}^n (a_i + I) t^i$$

$$f'(x + I) = \sum_{i=0}^n (a_i + I)(x + I)^i = \sum_{i=0}^n a_i x^i + I = \left(\sum_{i=0}^n a_i x^i \right) + I = f(x) + I \underbrace{=}_{f(x) \in I} I$$

e poiche' I e' lo zero di L , si ha che α e' proprio una radice di $f'(t)$.

(2) $\text{Dim. } \exists F', K : F \simeq F' \preceq K$

scegliendo $F' = \text{Im } \varphi$, $K = F'(\alpha)$ abbiamo

$$\varphi \text{ iniettiva} \Rightarrow F \simeq \text{Im } \varphi = F' \preceq F'(\alpha) = K$$

$$F \simeq F' \preceq K$$

(3) $\text{Dim dim}_{F'} K = n$

Se consideriamo la seguente restrizione di $\tilde{\varphi}$:

$$\tilde{\varphi} : F[t] \longrightarrow \text{Im } \tilde{\varphi}$$

otteniamo un isomorfismo ($\tilde{\varphi}$ e' iniettiva). Quindi,

$$n = \deg f(t) = \deg \tilde{\varphi}(f(t)) = \deg f'(t)$$

$$f(t) \text{ irriducibile} \Rightarrow f'(t) \text{ irriducibile}$$

Considerando il polinomio monico $\bar{f}'(t)$, ricavato da $f'(t)$, si ha

$$\begin{cases} \bar{f}'(\alpha) = 0 \\ \bar{f}'(t) \text{ monico} \\ \bar{f}'(t) \text{ irriducibile} \end{cases} \quad \underbrace{\Rightarrow}_{[2.30, \text{pg. 24}]} \quad \bar{f}'(\alpha) = P_{\min}(\alpha, F')$$

$$f'(\alpha) = 0 \Rightarrow \alpha \text{ algebrico in } F' \quad \underbrace{\Rightarrow}_{[2.40, \text{pg. 29}]} \quad \dim_{F'} F'(\alpha) = \deg P_{\min}(\alpha, K) = \deg \bar{f}'(\alpha) = n$$

$$\dim_{F'} F'(\alpha) = n \Leftrightarrow \dim_{F'} K = n$$

□

Proposition 2.49. *Sia*

1. F campo
2. $f(x) = a\bar{f}(x) \in F[x]$, $\bar{f}(x)$ monico
3. $n = \deg f(x) \geq 1$

allora

$$\exists F', K \text{ campi: } \begin{cases} F \simeq F' \preceq K \\ \dim_{F'} K \leq n! \\ \exists \alpha_1, \dots, \alpha_n \in K : f'(x) = a'(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \end{cases}$$

dove $f'(x), a'$ sono le immagini di $f(x), a$ tramite l'indotto dell'isomorfismo $F \simeq F'$.

In pratica, a meno di isomorfismi, riusciamo a trovare un campo K in cui $f'(x)$ si spezza linearmente.

Inoltre, si ha

$$f(x) \text{ riducibile in } F[x] \Rightarrow \dim_{F'} K < n!$$

o equivalentemente:

$$\dim_{F'} K \geq n! \Rightarrow f(x) \text{ irriducibile in } F[x]$$

ma poiche' $\dim_{F'} K \leq n!$, cio' vuol dire che:

$$\dim_{F'} K = n! \Rightarrow f(x) \text{ irriducibile in } F[x]$$

Proof: Chiameremo $P1$ la proposizione

$$f(x) \text{ riducibile in } F[x] \Rightarrow \dim_{F'} K < n!$$

Procediamo per induzione su n .

(1) $n = 1$

$$n = 1 \Rightarrow f(x) = a(x - \alpha_1) \in F[x]$$

Quindi, basta scegliere $K = F$, inoltre

$$\dim_F F = 1 \leq n! = 1! = 1$$

Poiche' $f(x)$ e' irriducibile, riguardo alla $P1$ non abbiamo nulla da dire.

(2) $n - 1 \Rightarrow n$

Sia $p(x) \in F[x]$ tale che

$$p(x) \nmid f(x) \Leftrightarrow f(x) = ap(x)h(x) \quad (*)$$

$$p(x) \text{ irriducibile in } F[x]$$

$$p(x), h(x) \text{ monici}$$

Nota: $p(x)$ esiste perche' $\deg f(x) = n \geq 1$.

$$(*) \Rightarrow \deg p(x) \leq n$$

Se $f(x)$ e' riducibile, possiamo scegliere $p(x)$ in modo da avere:

$$\deg p(x) < n \quad (*')$$

CASE: $\deg p(x) = 1$

$$\deg p(x) = 1 \Rightarrow p(x) = (x - \alpha_1), \alpha_1 \in F$$

$$\deg p(x) = 1 \underbrace{\Rightarrow}_{(*)} \deg h(x) = n - 1$$

Applicando l'ipotesi induttiva su $h(x)$, abbiamo allora

$$\exists K, F' : F \simeq F' \preceq K, \exists \alpha_2, \dots, \alpha_n \in K : h'(x) = (x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_n), \dim_{F'} K \leq (n - 1)! < n! \quad (+)$$

$$\Rightarrow f'(x) = a'p'(x)h'(x) = a'(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_n)$$

Nota: per la (+), la P1 e' vera.

CASE: $h = \deg p(x) > 1$

Per la prop [2.48,pg.34], applicata a $p(x)$, si ha

$$\exists F', K \text{ campi: } F \simeq F' \preceq K, \dim_{F'} K = h, \exists \alpha_1 \in K : p'(\alpha_1) = 0, p'(t) \in F'[t]$$

$$\alpha_1 \in K, p'(t) \in F'[t] \subseteq K[t], p'(\alpha_1) = 0 \underbrace{\Rightarrow}_{\text{Ruffini}} p'(t) = (t - \alpha_1)g'(t) \in K[t] \Rightarrow$$

$$\underbrace{\Rightarrow}_{(*)} f'(t) = a'(t - \alpha_1)g'(t)h'(t) \in K[t] \Rightarrow (**)$$

$$\Rightarrow \deg g'(t)h'(t) = n - 1 \Rightarrow$$

$$\underbrace{\Rightarrow}_{\text{Hp induttiva}} \exists \overline{K} : K \preceq \overline{K}, \exists \alpha_2, \dots, \alpha_n \in \overline{K} : g'(t)h'(t) = (x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_n), \dim_K \overline{K} \leq (n - 1)!$$

Hp induttiva

$$\underbrace{\Rightarrow}_{(**)} f'(x) = a'(t - \alpha_1)(x - \alpha_2)(x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_n)$$

Consideriamo:

$$F' \preceq K \preceq \overline{K}$$

$$\dim_{F'} K = h \underbrace{\leq}_{(*)} n \quad (++)$$

$$\dim_K \overline{K} \leq (n - 1)!$$

$$\dim_{F'} K \dim_K \overline{K} \leq n! \quad \underbrace{\Leftrightarrow}_{[2.18,pg.16]} \dim_{F'} \overline{K} \leq n!$$

Quindi $\overline{K}$ e' proprio il campo cercato.

Se $f(x)$ fosse stato riducibile, nella (++), avremmo potuto applicare la (*) al posto della (*), ottenendo cosi'

$$\begin{cases} \dim_{F'} K = h \underbrace{\leq}_{(*)'} n \\ \dim_K \overline{K} \leq (n - 1)! \end{cases} \Rightarrow \dim_{F'} K \dim_K \overline{K} < n! \Rightarrow \dim_{F'} \overline{K} < n!$$

quindi la P1 e' vera.

□

Definition 2.50. Sia

1. $F \preceq K$ estensione
2. $f(x) = a\bar{f}(x) \in F[x]$, $\bar{f}(x)$ monico
3. $n = \deg f(x)$

allora

$$K \text{ campo di spezzamento di } f(x) \text{ su } F \stackrel{\text{def}}{\iff} \begin{cases} 1. \exists \alpha_1, \dots, \alpha_n \in K : f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \\ 2. K = F(\alpha_1, \dots, \alpha_n) \end{cases}$$

La condizione 1. impone che $f(x)$ si spezzi linearmente in K , la 2. che K sia generato da F e da $\alpha_1, \dots, \alpha_n$.

Nota¹¹

Nota¹²

Per indicare che K e' un campo di spezzamento di $f(x)$ su F , scriveremo:

$$K = CS(f(x), F)$$

Proposition 2.51. Sia F campo, $f(x) \in F[x]$. A meno di isomorfismi, un campo di spezzamento K di $f(x)$ esiste, e $\dim_F K \leq n!$, con $n = \deg f(x)$.

Proof: Per la prop. [2.49,pg.36], si ha

$$\exists F', K \text{ campi: } \begin{cases} F \simeq F' \preceq K \\ \dim_{F'} K \leq n! \\ \exists \alpha_1, \dots, \alpha_n \in K : f'(x) = a'(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \end{cases}$$

Allora, per soddisfare la 2. della def. di campo di spezzamento, scegliamo direttamente $F(\alpha_1, \dots, \alpha_n)$ come campo di spezzamento. $\square$

Theorem 2.52. Sia

1. $F \preceq K$, $F' \preceq K'$ estensioni
2. $f(x) \in F[x]$, $f'(x) \in F'[x]$
3. $f'(x) = a'\bar{f}'(x) \in F'[x]$, $\bar{f}'(x)$ monico
4. $n = \deg f(x)$

allora

$$\begin{cases} \exists \psi : F \longrightarrow F' \text{ isomorfismo} \\ f'(x) = \tilde{\psi}(f(x)) \\ K = CS(f(x), F) \\ K' = CS(f'(x), F') \end{cases} \Rightarrow \begin{cases} \exists \Psi : K \simeq K' \text{ isomorf.} \\ \Psi|_F = \psi \end{cases}$$

¹¹poiche' $n = \deg f(x)$, per la 1. e per Ruffini (vedi [AI,16.1,pg.66]), $\alpha_1, \dots, \alpha_n$ sono tutte le radici di $f(x)$, anche se alcune potrebbero non essere distinte.

¹²Si ha

$$F(\alpha_1, \dots, \alpha_n) = F(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$$

dove $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ sono tutte le α_i , a due a due distinte, che non stanno in F .

dove $\tilde{\psi} : F[x] \longrightarrow F'[x]$ e' l'indotto di ψ , $\Psi|_F$ e' la restrizione di Ψ a F .
Possiamo rappresentare il thm graficamente:

$$\begin{array}{ccc} \begin{array}{c} K \\ \downarrow \psi \\ F \end{array} & \begin{array}{c} K' \\ \downarrow \psi \\ F' \end{array} & \Rightarrow \begin{array}{ccc} K & \xrightarrow{\Psi} & K' \\ \downarrow \psi & & \downarrow \psi \\ F & \xrightarrow{\psi} & F' \end{array} \end{array}$$

Proof: Sia $\tilde{\psi} : F[x] \longrightarrow F'[x]$ l'isomorfismo¹³ indotto da ψ .
Osserviamo che poiche' $\tilde{\psi}$ e' un isomorfismo, si ha

$$n = \deg f(x) = \deg f'(x)$$

Sia $m = \dim_F K$. Lavoriamo per induzione su m .

(1) $m = 1$

$$\left\{ \begin{array}{l} \dim_F K = m = 1 = \dim_F F \\ F \subseteq K \text{ sottospazio vett.} \end{array} \right. \xRightarrow{[\text{AL}, 4.10.2, \text{pg.27}]} F = K$$

$$\begin{aligned} F = K = CS(f(x), F) &\Rightarrow f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \xrightarrow{\tilde{\psi}} f'(x) = a'(x - \alpha'_1)(x - \alpha'_2) \dots (x - \alpha'_n) \in F'[x] \\ K' = CS(f'(x), F') &= F'(\alpha'_1, \dots, \alpha'_n) \underbrace{=}_{\alpha'_i \in F'} F' \end{aligned}$$

$$K = F \xrightarrow{\psi} F' = K'$$

$$K \simeq K', \quad \psi|_F = \psi$$

(2) Tesi induttiva: $\forall h < m \Rightarrow m$

Supponiamo $m > 1$ (dato che per $m = 1$ abbiamo gia' dimostrato la tesi).

(2.1) $\exists p(x) \in F[x] : \deg p(x) > 1, p(x) \nmid f(x), p(x)$ irriducibile, monico

Se per assurdo, tutti i fattori di $f(x)$ fossero del tipo $x - \alpha \in F[x]$, allora $f(x)$ si spezzerebbe linearmente in $F[x]$, ovvero, tutte le sue radici $\alpha_1, \dots, \alpha_n \in F$, e quindi

$$K = CS(f(x), F) = F(\alpha_1, \dots, \alpha_n) \underbrace{=}_{\alpha_i \in F} F$$

$$K = F \Rightarrow \dim_F K = \dim_F F = 1 \Leftrightarrow m = 1 \text{ assurdo contro } m > 1$$

Quindi deve esistere almeno un suo fattore irriducibile, di grado > 1 . Questo fattore si puo' poi rendere monico. Sia $p(x)$ un tale fattore.

(2.2) Sia $h = \deg p(x)$, si ha

$$n \geq h > 1$$

$$n \underbrace{\geq}_{p(x) \nmid f(x)} h \underbrace{>}_{2.1} 1 \quad (1)$$

Sia $p'(x) = \tilde{\psi}(p(x))$.

$$(2.3) \exists \alpha \in K : \frac{F[x]}{(p(x))} \simeq F[\alpha] = F(\alpha), \quad P_{\min}(\alpha, F) = p(x)$$

$$K = CS(f(x), F) \Rightarrow f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \in K[x] \quad (2)$$

$$p(x) \nmid f(x) \Rightarrow f(x) = p(x)h(x) \quad (3)$$

¹³e' un isomorfismo poiche' ψ lo e' (vedi [1.13,pg.3])

Se per assurdo $\forall i \ h(\alpha_i) = 0$, allora $h(x)$ avrebbe grado $\geq n$, e per la (3), $p(x)$ avrebbe grado 0. Assurdo contro $h > 1$ la (1). Quindi

$$\exists \alpha = \alpha_{\bar{i}} : f(\alpha) = 0, \ h(\alpha) \neq 0 \underbrace{\Rightarrow}_{(3)} p(\alpha) = 0$$

allora

$$\begin{cases} p(x) \text{ irriducibile in } F[x] \\ p(\alpha) = 0 \\ p(x) \text{ monico} \end{cases} \underbrace{\Rightarrow}_{[2.30, \text{pg. } 24]} p(x) = P_{\min}(\alpha, F), \quad \frac{F[x]}{(p(x))} \simeq F[\alpha] \underbrace{=}_{[2.36, \text{pg. } 27]} F(\alpha)$$

$$(2.4) \ \exists \alpha' \in K' : \frac{F'[x]}{(p'(x))} \simeq F'[\alpha'] = F'(\alpha')$$

Basta ripetere la dimostrazione dei passi 2.1, 2.3, utilizzando $f'(x), p'(x), F', K'$ al posto di $f(x), p(x), F, K$

$$(2.5) \ \frac{F[x]}{(p(x))} \simeq \frac{F'[x]}{(p'(x))}$$

Consideriamo il seguente omomorfismo:

$$F[x] \xrightarrow{\tilde{\psi}} F'[x] \xrightarrow{\pi} \frac{F'[x]}{(p'(x))}$$

dove π e' la suriezione naturale.

$\pi \circ \tilde{\psi}$ e' un omomorfismo surriettivo perche' $\tilde{\psi}$ e' un isomorfismo e π e' surriettivo. Allora, per il thm dell'omomorfismo [AI, 17.10.1, pg. 86], si ha

$$\frac{F[x]}{\ker \pi \circ \tilde{\psi}} \simeq \frac{F'[x]}{(p'(x))}$$

$$\begin{aligned} \ker \pi \circ \tilde{\psi} &= \left\{ g(x) \in F[x] \mid \tilde{\psi}(g(x)) + \langle p'(x) \rangle = \langle p'(x) \rangle \Leftrightarrow \tilde{\psi}(g(x)) \in \langle p'(x) \rangle \right\} = \\ &= \left\{ g(x) \in F[x] \mid \tilde{\psi}(g(x)) \in \langle p'(x) \rangle \right\} = \tilde{\psi}^{-1}(\langle p'(x) \rangle) = \left\langle \tilde{\psi}^{-1}(p'(x)) \right\rangle \underbrace{=}_{\tilde{\psi} \text{ isomorfismo, } p'(x) = \tilde{\psi}(p(x))} \langle p(x) \rangle \end{aligned}$$

$$\frac{F[x]}{(p(x))} \simeq \frac{F'[x]}{(p'(x))}$$

$$(2.6) \ \exists \tau : F(\alpha) \longrightarrow F'(\alpha') \text{ isomorfismo t.c. } \tau|_F = \psi$$

Dai passi 2.3, 2.4, 2.5, segue che:

$$F(\alpha) = F[\alpha] \simeq \frac{F[x]}{(p(x))} \simeq \frac{F'[x]}{(p'(x))} \simeq F'[\alpha'] = F'(\alpha')$$

$$F(\alpha) \simeq F'(\alpha')$$

Sia $\tau : F(\alpha) \longrightarrow F'(\alpha')$ tale isomorfismo. Esaminando gli isomorfismi fin'ora usati, τ risulta essere:

$$\begin{aligned} f(\alpha) \in F[\alpha] &\mapsto \tilde{\psi}(f(\alpha')) \in F'[\alpha'] \\ \Rightarrow a \in F &\leq F[\alpha] \mapsto \tilde{\psi}(a) = \psi(a) \in F' \\ \Rightarrow \tau|_F &= \psi \end{aligned}$$

$$(2.7) \ K = CS(f(x), F(\alpha)), \ [K : F(\alpha)] < m$$

$$K = CS(f(x), F) = F(\alpha_1, \dots, \alpha_n) \underbrace{=}_{\alpha = \alpha_{\bar{i}}, [2.22, \text{pg. } 19]} F(\alpha)(\alpha_1, \dots, \alpha_{\bar{i}-1}, \alpha_{\bar{i}+1}, \dots, \alpha_n)$$

e poiche' $f(x) \in F(\alpha)[x]$, proprio per definizione, si ha

$$F(\alpha)(\alpha_1, \dots, \alpha_{\bar{i}-1}, \alpha_{\bar{i}+1}, \dots, \alpha_n) = CS(f(x), F(\alpha))$$

Infine,

$$\dim_F F(\alpha) \underbrace{=}_{[2.40, \text{pg.29}]}} \deg P_{\min}(\alpha, F) \underbrace{=}_{2.3}} \deg p(x) = h \underbrace{>}_{2.2}} 1$$

$$\dim_F F(\alpha) = r > 1$$

$$\dim_F K = m$$

$$[K : F(\alpha)][F(\alpha) : F] \underbrace{=}_{[2.18, \text{pg.16}]}} [K : F] \Leftrightarrow [K : F(\alpha)] = \frac{m}{r} \underbrace{<}_{r>1}} m$$

$$\langle 2.8 \rangle \quad K' = CS(f'(x), F'(\alpha'))$$

Analogamente a prima.

$\langle 2.9 \rangle$ Q.E.D.

Riassumiamo graficamente la situazione:

$$\begin{array}{ccc} K & & K' \\ | & & | \\ F(\alpha) & \rightsquigarrow^{\tau} & F'(\alpha') \end{array}$$

e poiche' $[K : F(\alpha)] < m$, possiamo applicare l'Hp induttiva, ottenendo:

$$\begin{array}{ccc} K & \rightsquigarrow^{\Psi} & K' \\ | & & | \\ F(\alpha) & \rightsquigarrow^{\tau} & F'(\alpha') \end{array}$$

e inoltre,

$$\Psi|_{F(\alpha)} = \tau \underbrace{\Rightarrow}_{F \subseteq F(\alpha)}} \Psi|_F = \tau|_F \underbrace{=}_{2.6}} \psi$$

□

Corollary 2.53. *Sia $f(x) \in F[x]$, allora il campo di spezzamento di $f(x)$ in F e' unico, a meno di isomorfismi, ovvero,*

$$\begin{cases} K_1 = CS(f(x), F) \\ K_2 = CS(f(x), F) \end{cases} \Rightarrow K_1 \simeq K_2$$

ed e' quindi lecito considerare la scrittura

$$K = CS(f(x), F)$$

come una effettiva identita'.

Nota ¹⁴.

Proof: Basta applicare il thm [2.52,pg.38], scegliendo

$$F' = F, \psi = \text{id}, K' = K_2$$

□

¹⁴Nella definizione [2.50,pg.38] avevamo detto che la scrittura

$$K = CS(f(x), F)$$

indicava K come *un qualsiasi* campo di spezzamento di $f(x)$ in F . Adesso, invece, possiamo dire che $CS(f(x), F)$ e' il campo di spezzamento di $f(x)$ in F , ed e' quindi corretto scrivere:

$$K \simeq CS(f(x), F)$$

che per convenzione, scriveremo come

$$K = CS(f(x), F)$$

Proposition 2.54. Dato $f(x) \in F[x]$,

$$\begin{cases} K = CS(f(x), F) \\ F \preceq L \preceq K \end{cases} \Rightarrow K = CS(f(x), L)$$

Proof: Siano $\alpha_1, \dots, \alpha_n$ tutte le radici di $f(x)$

$$\begin{aligned} K = CS(f(x), F) &= F(\alpha_1, \dots, \alpha_n) \underbrace{\subseteq}_{F \subseteq L} L(\alpha_1, \dots, \alpha_n) \underbrace{\subseteq}_{L \subseteq K} K(\alpha_1, \dots, \alpha_n) \underbrace{=}_{\alpha_i \in K} K \\ K &= L(\alpha_1, \dots, \alpha_n) = CS(f(x), L) \end{aligned}$$

□

2.4 Campi chiusi e chiusura

Definition 2.55. Sia F un campo.

$$F \text{ e' algebricamente chiuso} \stackrel{\text{def}}{\Leftrightarrow} \forall f(x) \in F[x] : \deg f(x) \geq 1 \quad \exists \alpha \in F : f(\alpha) = 0$$

Proposition 2.56. Sia F un campo. Le seguenti proposizioni sono equivalenti:

1. F e' algebricamente chiuso
2. $\forall f(x) \in F[x] : \deg f(x) \geq 1 \quad f(x)$ si spezza linearmente in F
3. $f(x) \in F[x]$ irriducibile in $F \Leftrightarrow \deg f(x) = 1$
4. $F \preceq K$ estensione algebrica $\Leftrightarrow F = K$

Proof:

(1) $1. \Leftrightarrow 2.$

$$F \text{ chiuso} \Rightarrow \exists \alpha \in F : f(\alpha) = 0 \quad \underbrace{\Rightarrow}_{\text{thm di Ruffini [AI, 16.1, pg. 66]}} \quad f(x) = (x - \alpha)g(x), \quad g(x) \in F[x]$$

$$\deg f(x) = \deg(x - \alpha)g(x) = 1 + \deg g(x)$$

$$\deg g(x) = \deg f(x) - 1$$

Procediamo per induzione su $n = \deg f(x)$.

CASE: $n = 1$

$$\deg f(x) = \deg(x - \alpha)g(x) = 1 + \deg g(x)$$

$$\deg f(x) = 1 \Rightarrow \deg g(x) = 0 \Rightarrow f(x) = c(x - \alpha)$$

CASE: $n - 1 \Rightarrow n$

$$\deg g(x) = n - 1 \quad \underbrace{\Rightarrow}_{\text{Hp indutt.}} \quad g(x) = (x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_n), \quad \alpha_i \in F \quad \forall i = 2, \dots, n$$

Il viceversa e' immediato.

(2) $1. \Leftrightarrow 3.$

(2.1) Dim. $\Rightarrow$

Sia $f(x) \in F[x]$ irriducibile. Per definizione $\deg f(x) \geq 1$ (in quanto $f(x)$ non e' invertibile).

Se per assurdo $\deg f(x) > 1$, allora

$$F \text{ chiuso} \Rightarrow \exists \alpha \in F : f(\alpha) = 0 \quad \underbrace{\Rightarrow}_{\text{Ruffini}} \quad f(x) = (x - \alpha)g(x)$$

$$\deg f(x) > 1 \Rightarrow \deg g(x) > 0 \Rightarrow f(x) \text{ riducibile. Assurdo.}$$

(2.1) Dim. $\Leftarrow$

Sia $f(x) \in F[x]$, con $\deg f(x) \geq 1$.

Procediamo per induzione su $n = \deg f(x)$.

Se $n = 1$, allora $f(x) = x - \alpha \in F[x]$, e quindi $f(\alpha) = 0$.

Se $\deg f(x) > 1$, per la 3., $f(x)$ e' riducibile in $F[x]$:

$$f(x) = g(x)h(x), \quad g(x), h(x) \in F[x], \quad 1 \leq \deg g(x) < n$$

Per Hp induttiva $\exists \alpha \in F : g(\alpha) = 0 \Rightarrow f(\alpha) = 0$

(2.1) Dim 2. $\Rightarrow$ 4.

Sia $F \preceq K$ una estensione algebrica e sia $\alpha \in K$, allora

$$\alpha \in K \quad \underbrace{\Rightarrow}_{F \preceq K \text{ algebrica}} \quad \exists f(x) \in F[x] \setminus \{0\} : f(\alpha) = 0$$

$$f(\alpha) = 0, \quad f \neq 0 \Rightarrow \deg f \geq 1$$

Per la 2., tutte le radici di $f(x)$ stanno in F e quindi

$$\alpha \in F$$

Per l'arbitrarieta' di α abbiamo

$$K \subseteq F$$

e poiche' $F \subseteq K$, si ha $F = K$.

(2.2) 4. $\Rightarrow$ 1.

Sia $f(x) \in F[x] : \deg f(x) \geq 1$.

Per la prop [2.48,pg.34], si ha

$$\exists K : F \subseteq K \quad \exists \alpha \in K : f(\alpha) = 0 \Rightarrow \alpha \text{ algebrico in } F \Rightarrow$$

$$\underbrace{\Rightarrow}_{[2.43,pg.31]} \quad F \preceq F(\alpha) \text{ e' algebrica} \quad \underbrace{\Rightarrow}_4 \quad F = F(\alpha) \Rightarrow \alpha \in F$$

Abbiamo quindi trovato un $\alpha \in F : f(\alpha) = 0$.

□

Definition 2.57. Sia $F \preceq \overline{F}$ una estensione. Poniamo

$$\overline{F} \text{ si chiama chiusura algebrica di } F \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \begin{cases} F \preceq \overline{F} \text{ estensione algebrica} \\ \overline{F} \text{ algebricamente chiuso} \end{cases}$$

Lemma 2.58. Sia

1. $F \preceq L \preceq K = L(\alpha)$, con $\alpha \in K$ algebrico su L
2. $p(x) = P_{\min}(\alpha, L)$, $n = \deg p(x)$
3. $\varphi : L \longrightarrow \overline{F}$ una immersione
4. $\Phi : L[x] \longrightarrow \overline{F}[x]$ l'omomorfismo indotto da φ (vedi [1.13,pg.3]), ovvero

$$\Phi : L[x] \longrightarrow \overline{F}[x]$$

$$\sum_{i=0}^r a_i x^i \mapsto \sum_{i=0}^r \varphi(a_i) x^i$$

5. Sia $\overline{\beta}$ una radice di $\Phi(p)$

6. Sia data la seguente legge:

$$f : K = L(\alpha) \longrightarrow \overline{F}$$

$$b_0 + b_1 \alpha + b_2 \alpha^2 + \cdots + b_{n-1} \alpha^{n-1} \mapsto \varphi(b_0) + \varphi(b_1) \overline{\beta} + \varphi(b_2) \overline{\beta}^2 + \cdots + \varphi(b_{n-1}) \overline{\beta}^{n-1}$$

o equivalentemente:

$$\begin{aligned} h(x) &\in L[x] \\ f(h(\alpha)) &= \Phi(h)(\bar{\beta}) \end{aligned}$$

Allora,

$$f \text{ e' un omomorfismo t.c. } f|_L = \varphi$$

Proof:

(1) f e' ben posta

$$\begin{aligned} \text{Im } \varphi \subseteq \bar{F} \\ \left\{ \begin{array}{l} \bar{\beta} \text{ radice di } \Phi(p) \\ \Phi(p) \in \bar{F}[x] \\ \bar{F} \text{ chiuso} \end{array} \right. \Rightarrow \bar{\beta} \in \bar{F} \end{aligned}$$

$$\Rightarrow \varphi(b_0) + \varphi(b_1)\bar{\beta} + \varphi(b_2)\bar{\beta}^2 + \cdots + \varphi(b_{n-1})\bar{\beta}^{n-1} \in \bar{F}$$

(2) f e' una funzione ben definita e le sue due definizioni date nelle Hp sono equivalenti

$$K = L(\alpha), \quad \alpha \text{ algebrico su } L \quad \underbrace{\Rightarrow}_{[2.40, \text{pg. 29}]} \quad \{1, \alpha, \dots, \alpha^{n-1}\} \text{ e' una base di } K_L$$

Quindi ogni elemento di K si scrive in modo unico come

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}, \quad b_i \in L \quad \forall i$$

e questo garantisce che

$$b, c \in K, \quad b = c \Rightarrow f(b) = f(c)$$

Inoltre,

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

$$f(h(\alpha)) = f(b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}) = \varphi(b_0) + \varphi(b_1)\bar{\beta} + \varphi(b_2)\bar{\beta}^2 + \cdots + \varphi(b_{n-1})\bar{\beta}^{n-1} = \Phi(h)(\bar{\beta})$$

(3) $f|_L = \varphi$

$$c \in L \Rightarrow c = b_0 \Rightarrow f(c) = f(b_0) = \varphi(b_0) = \varphi(c)$$

(4) f e' un omomorfismo

$$(4.1) \quad f(c + d) = f(c) + f(d)$$

$$c, d \in K = L(\alpha) \Rightarrow \exists s(x), t(x) \in L[x] : \quad c = s(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i, \quad d = t(\alpha) = \sum_{i=0}^{n-1} d_i \alpha^i$$

$$c + d = \sum_{i=0}^{n-1} (c_i + d_i) \alpha^i$$

$$f(c + d) = \sum_{i=0}^{n-1} \varphi(c_i + d_i) \bar{\beta}^i \quad \underbrace{=}_{\varphi \text{ omomorf.}} \quad \sum_{i=0}^{n-1} (\varphi(c_i) + \varphi(d_i)) \bar{\beta}^i = \sum_{i=0}^{n-1} \varphi(c_i) \bar{\beta}^i + \sum_{i=0}^{n-1} \varphi(d_i) \bar{\beta}^i = f(c) + f(d)$$

(4.2) Dim. che $f(cd) = f(c)f(d)$.

Dividiamo $s(x)t(x)$ per $p(x)$ (in $L[x]$):

$$st = pq + r, \quad r(x) = \sum_{i=0}^{n-1} r_i x^i \in L[x]$$

$$cd = s(\alpha)t(\alpha) = p(\alpha)q(\alpha) + r(\alpha) \underbrace{\quad}_{p(\alpha)=0} r(\alpha)$$

$$f(cd) = f(r(\alpha)) \underbrace{\quad}_{\text{per def.}} \Phi(r)(\bar{\beta})$$

$$\bar{\beta} \text{ radice di } \Phi(p) \Rightarrow \Phi(p)(\bar{\beta}) = 0 \quad (*)$$

$$\begin{aligned} f(cd) &= \Phi(r)(\bar{\beta}) \underbrace{\quad}_{(*)} \Phi(r)(\bar{\beta}) + \Phi(p)(\bar{\beta})\Phi(q)(\bar{\beta}) \underbrace{\quad}_{\Phi \text{ omomorfismo}} \Phi(r + pq)(\bar{\beta}) = \Phi(st)(\bar{\beta}) = \\ &\underbrace{\quad}_{\Phi \text{ omomorfismo}} \Phi(s)(\bar{\beta})\Phi(t)(\bar{\beta}) \underbrace{\quad}_{\text{per def.}} f(s(\alpha))f(t(\alpha)) = f(c)f(d) \end{aligned}$$

□

Theorem 2.59. *Sia F un campo, allora*

1. $\exists \bar{F}$ chiusura algebrica di F
2. $F \preceq K$ estensione algebrica $\Rightarrow \exists \varphi : K \hookrightarrow \bar{F}, \quad \varphi|_F = \text{id}$
3. Due chiusure algebriche di F sono isomorfe.

Grazie alla 3., esiste un'unica chiusura algebrica di F (a meno di isomorfismi), che indicheremo con $\bar{F}$.

Proof:

(1) Dim 1.

Sia

$$\mathcal{F} = \{K \text{ campo} \mid F \preceq K \text{ estensione algebrica} \}$$

(1.1) $(\mathcal{F}, \preceq)$ e' un POSET, dove $\preceq$ e' l'inclusione di campi

Siano $F, K, J \in \mathcal{F}$

1. $F \preceq F$
2. $F \preceq K, K \preceq F \Rightarrow F = K$
3. $F \preceq K \preceq J \Rightarrow F \preceq J$

(1.2) $\exists \bar{F}$ elemento massimale in $\mathcal{F}$

Cerchiamo di applicare il lemma di Zorn (vedi [1.21,pg.7]).

Sia $\{K_i\}_{i \in I} \subseteq \mathcal{F}$ una catena in $\mathcal{F}$ e consideriamo

$$J = \bigcup_{i \in I} K_i$$

(1.2.1) J e' un maggiorante delle catena

Chiaramente $K_i \subseteq J \quad \forall i \in I$.

Resta da dimostrare che $J \in \mathcal{F}$.

J e' un campo:

$$a \in J, b \in J^* \Rightarrow \exists K_i, K_j : a \in K_i \vee b \in K_j$$

$$\{K_i\} \text{ e' una catena} \Rightarrow K_i \preceq K_j \vee K_j \preceq K_i$$

$$K_i \subseteq K_j \Rightarrow a + b, ab, -a, b^{-1} \in K_j \subseteq J$$

$$K_j \subseteq K_i \Rightarrow a + b, ab, -a, b^{-1} \in K_i \subseteq J$$

Quindi J e' un campo.

$F \preceq J$ e' algebrica:

$$\alpha \in J \Rightarrow \exists K_i : \alpha \in K_i \quad \underbrace{\Rightarrow}_{F \preceq K_i \text{ algebrica}} \quad \exists f(x) \in F[x] \setminus \{0\} : F(\alpha) = 0$$

$$\Rightarrow F \preceq J \text{ e' algebrica}$$

In definitiva, $J \in \mathcal{F}$.

Abbiamo cosi' visto che ogni catena in $\mathcal{F}$ ha un maggiorante J , allora per il lemma di Zorn (vedi [1.21,pg.7]), $\exists \bar{F} \in \mathcal{F}$ massimale.

(1.3) $\bar{F}$ e' una chiusura di F

Utilizziamo la 4. della prop. [2.56,pg.42]: sia $\bar{F} \preceq K$ una estensione algebrica di $\bar{F}$. Dimostriamo che $\bar{F} = K$.

$$\bar{F} \in \mathcal{F} \Rightarrow F \preceq \bar{F} \text{ algebrica}$$

$$\bar{F} \preceq K \text{ algebrica}$$

$$\underbrace{\Rightarrow}_{[2.45,pg.31]} F \preceq K \text{ algebrica} \Rightarrow K \in \mathcal{F}$$

$$\begin{cases} K \in \mathcal{F} \\ \bar{F} \subseteq K \\ \bar{F} \text{ massimale in } \mathcal{F} \end{cases} \Rightarrow \bar{F} = K$$

(2) Dim 2.

Useremo ancora una volta il lemma di Zorn.

Sia

$$S = \{(L, \varphi) \mid F \preceq L \preceq K, \varphi : L \longrightarrow \bar{F} \text{ omomorfismo t.c. } \varphi|_F = \text{id}\}$$

e definiamo la seguente relazione su S :

$$(L, \varphi) \leq (L', \varphi') \Leftrightarrow \begin{cases} L \subseteq L' \\ \varphi'|_L = \varphi \end{cases}$$

(2.1) $(S, \leq)$ e' un POSET

1. $(L, \varphi) \leq (L, \varphi)$

2. antisimmetria:

$$(L, \varphi) \leq (L', \varphi'), (L', \varphi') \leq (L, \varphi) \Rightarrow \begin{cases} L = L' \\ \varphi = \varphi'|_L = \varphi'|_{L'} = \varphi' \end{cases} \Rightarrow (L, \varphi) = (L', \varphi')$$

3. transitivita':

$$\begin{cases} L \preceq L' \preceq L'' \\ (\varphi''|_{L'} = \varphi')|_L = \varphi \end{cases}$$

(2.2) Sia $\{(L_i, \varphi_i)\}_{i \in I}$ una catena di elementi di S . Dimostriamo che un maggiorante e'

(L, φ) , dove

$$L = \bigcup_{i \in I} L_i$$

$$\varphi(x) = \varphi_i(x) \text{ se } x \in L_i$$

Chiaramente

$$\begin{cases} L_i \subseteq L \\ \varphi|_{L_i} = \varphi_i \end{cases}$$

resta da dimostrare che $(L, \varphi) \in S$

$$F \subseteq L_i \subseteq L = \bigcup L_i \underbrace{\subseteq}_{L_i \subseteq K \ \forall i} K$$

L e' un campo:

$$a_i \in L_i, b_i \in L_j \Rightarrow a_i \pm b_i, a_i b^{-1}_i \in \begin{cases} L_i & L_i \supseteq L_j \\ L_j & L_j \supseteq L_i \end{cases} \subseteq L$$

$$\Rightarrow F \preceq L \preceq K$$

φ e' ben definita su tutto L (poiche' $L = \bigcup L_i$)

φ e' un omomorfismo:

$$\varphi(a_i + b_j) = \begin{cases} \varphi_i(a_i + b_j) = \varphi_i(a_i) + \varphi_i(b_j) & L_i \supseteq L_j \\ \varphi_j(a_i + b_j) = \varphi_j(a_i) + \varphi_j(b_j) & L_j \supseteq L_i \end{cases} = \varphi(a_i) + \varphi(b_j)$$

analogamente per il prodotto

Abbiamo cosi' visto che ogni catena di elementi di S ammette un maggiorante in S , quindi per il lemma di Zorn (vedi [1.21,pg.7]) esiste un elemento (M, ϕ) massimale in S .

(2.3) Dim. che $M = K$

$$(M, \phi) \in S \Rightarrow \begin{cases} F \preceq M \preceq K \\ \phi : M \longrightarrow \overline{F} \end{cases}$$

Poiche' $M \subseteq K$, basta dimostrare che $K \subseteq M$. Supponiamo per assurdo che $K \not\subseteq M$, ovvero che $\exists \alpha \in K : \alpha \notin M$.

$$\alpha \notin M \Rightarrow M \subsetneq M(\alpha)$$

Cercheremo adesso un elemento $(M(\alpha), f)$ che contrasta con la massimalita' di (M, ϕ) .

Osserviamo che

$$\begin{cases} F \preceq K \text{ algebrica} \\ F \preceq M \preceq K \end{cases} \underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} M \preceq K \text{ algebrica} \Rightarrow \alpha \in K \text{ e' algebrico su } M \quad (*)$$

$$\phi|_F = \text{id}, \quad 1 \underbrace{\in}_{[1.1, \text{pg.1}]} M \Rightarrow \text{Im } \phi = \phi(M) \neq \{0\} \quad \underbrace{\Rightarrow}_{[\text{AI}, 18.2, \text{pg.90}]} \phi \text{ e' una immersione} \quad (**)$$

Sia data la seguente legge:

$$f : M(\alpha) \longrightarrow \overline{F}$$

$$h(x) \in M[x]$$

$$f(h(\alpha)) = \tilde{\phi}(h)(\overline{\beta})$$

dove

$$\tilde{\phi} : M[x] \longrightarrow \overline{F}[x] \text{ e' l'indotto di } \phi \text{ vedi [1.13,pg.3]}$$

$$p(x) = P_{\min}(\alpha, M) \quad \text{che esiste per la } (*)$$

$$\overline{\beta} \text{ radice di } \tilde{\phi}(p)$$

Per il lemma [2.58,pg.43] si ha che

$$f \text{ e' un omomorfismo t.c. } f|_M = \phi \quad (1)$$

Quindi

$$\left\{ \begin{array}{l} f : M(\alpha) \longrightarrow \overline{F} \text{ omomorfismo} \\ f|_F \underbrace{=}_{(1), F \subseteq M} \phi|_F = \text{id} \\ F \preceq M \preceq M(\alpha) \underbrace{\preceq}_{M \subseteq K, \alpha \in K} K \end{array} \right. \Rightarrow (M(\alpha), f) \in S$$

$$\left\{ \begin{array}{l} M \subseteq M(\alpha) \\ f|_M = \phi \\ (M, \phi), (M(\alpha), f) \in S \end{array} \right. \Rightarrow (M, \phi) \leq (M(\alpha), f) \underbrace{\Rightarrow}_{(M, \phi) \text{ massimale}} (M, \phi) = (M(\alpha), f) \Rightarrow M = M(\alpha) \Rightarrow \alpha \in M$$

e questo e' assurdo contro $\alpha \notin M$.

Abbiamo cosi' visto che

$$\begin{aligned} K &= M \\ \phi : M = K &\longrightarrow \overline{F} \\ \phi|_F &= \text{id} \\ \phi &\text{ e' una immersione (per la (**))} \end{aligned}$$

Quindi la φ cercata e' proprio ϕ .

(3) Dim 3.

Supponiamo che K e $\overline{F}$ siano due chiusure algebriche di F , allora
 $F \preceq K$ e' algebrica

e quindi, per la 2.

$$\exists \varphi : K \longrightarrow \overline{F} \text{ immersione t.c. } \varphi|_F = \text{id}$$

dimostriamo che φ e' surriettiva, ovvero che $\overline{F} = \text{Im } \varphi$.

Sia $\gamma \in \overline{F}$

$$\begin{aligned} F \preceq \overline{F} \text{ algebrica} &\Rightarrow \exists p(x) = P_{\min}(\gamma, F) \\ \left\{ \begin{array}{l} p(x) \in F[x] \subseteq K[x] \\ K \text{ chiuso} \\ \gamma \text{ radice di } p(x) \end{array} \right. &\Rightarrow \gamma \in K \simeq \text{Im } \varphi \\ &\Rightarrow \overline{F} \subseteq K \simeq \text{Im } \varphi \\ F \preceq \overline{F} \preceq K &\Rightarrow \dim_F \overline{F} \leq \dim_F K \underbrace{=}_{(*)} \dim_F \text{Im } \varphi \\ F \subseteq \text{Im } \varphi \subseteq \overline{F} &\Rightarrow \dim_F \overline{F} \geq \dim_F \text{Im } \varphi \\ \left\{ \begin{array}{l} \text{Im } \varphi \subseteq \overline{F} \\ \dim_F \overline{F} = \dim_F \text{Im } \varphi \end{array} \right. &\Rightarrow \overline{F} = \text{Im } \varphi \end{aligned}$$

Nota(*) $\varphi|_F = \text{id} \Rightarrow F \subseteq \text{Im } \varphi$, quindi $\text{Im } \varphi$ e' un F spazio vettoriale, inoltre φ e' un applicazione lineare perche' $\varphi|_F = \text{id}$ (vedi [2.15,pg.15]).

□

Example 2.60.

1. $\mathbb{C} = \overline{\mathbb{R}}$, infatti

$$\begin{array}{ccc} \mathbb{R} & \underbrace{\preceq}_{[2.17, \text{pg.16}]} & \mathbb{C} \text{ e' finita} & \underbrace{\Rightarrow}_{[2.44, \text{pg.31}]} & \mathbb{R} \preceq \mathbb{C} \text{ algebrica} \\ & & \mathbb{C} \text{ e' chiuso vedi [6.39, pg.109]} & & \end{array}$$

quindi $\mathbb{C} = \overline{\mathbb{R}}$.

2. $\mathbb{C} \neq \overline{\mathbb{Q}}$, infatti, anche se $\mathbb{C}$ e' chiuso, l'estensione $\mathbb{Q} \subseteq \mathbb{C}$ non e' algebrica: basta considerare e, π che sono trascendenti su $\mathbb{Q}$.

Proposition 2.61. *Sia*

1. $F \preceq K$ una estensione algebrica

2. $\forall f(x) \in F[x] : \deg f(x) \geq 1 \quad f(x)$ si spezza linearmente in K

allora

$$K = \overline{F}$$

Proof: Poiche' per Hp $F \preceq K$ e' una estensione algebrica, basta dimostrare che K e' algebricamente chiuso. Usiamo direttamente la definizione.

Sia $f(x) \in K[x] : \deg f(x) \geq 1$. Per la prop [2.48, pg.34], si ha

$\exists L'$ campo : $K \preceq L', \exists \alpha \in L' : f(\alpha) = 0$

Sia $L = K(\alpha)$

$$f(\alpha) = 0 \Rightarrow \alpha \text{ algebrico in } K \quad \underbrace{\Rightarrow}_{[2.43, \text{pg.31}]} \quad K \preceq K(\alpha) \text{ algebrica}$$

$$\left\{ \begin{array}{l} F \preceq K \preceq K(\alpha) \\ F \preceq K \text{ algebrica} \\ K \preceq K(\alpha) \text{ algebrica} \end{array} \right. \quad \underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} \quad F \preceq K(\alpha) \text{ algebrica} \Rightarrow \alpha \text{ algebrico in } F \Rightarrow \exists p(x) := P_{\min}(\alpha, F)$$

$$p(x) \in F[x] \quad \underbrace{\Rightarrow}_{\text{Hp}} \quad p(x) = \prod_{i=1}^{\deg p} (x - \alpha_i), \quad \alpha_i \in F \quad \forall i = 1, \dots, \deg p$$

$$p(\alpha) = 0 \Rightarrow \exists \alpha_j : \alpha - \alpha_j = 0 \Leftrightarrow \alpha = \alpha_j \in F$$

Abbiamo cosi' trovato un $\alpha \in F : f(\alpha) = 0$. □

Proposition 2.62. *Sia $F \preceq K$ una estensione, allora*

$$F \preceq K \text{ algebrica} \Rightarrow \overline{K} = \overline{F}$$

Proof:

$$\underbrace{F \preceq K}_{\text{algebrica}}, \underbrace{K \preceq \overline{K}}_{\text{algebrica}} \quad \underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} \quad F \preceq \overline{K} \text{ algebrica}$$

Allora, poiche' $\overline{K}$ e' chiuso, per definizione si ha che $\overline{K}$ e' la chiusura algebrica di F , ovvero $\overline{k} = \overline{F}$. □

Proposition 2.63. *Sia $F \preceq K$ estensione, si ha*

$$K \text{ chiuso} \Rightarrow \overline{F} = \{\alpha \in K \mid \alpha \text{ algebrico su } F\}$$

Proof: Sia G il secondo insieme. Dobbiamo dimostrare che $\overline{F} = G$.

Intanto, per la prop [2.46,pg.33], G e' un campo. Sia $f(x) \in G[x] : \deg f(x) \geq 1$,

$$f(x) \in G[x] \subseteq K[x] \xRightarrow{K \text{ chiuso}} \exists \alpha \in K : f(\alpha) = 0$$

$$a \in F \Rightarrow a \text{ algebrico in } F \text{ (basta considerare } x - a) \Rightarrow a \in G \\ \Rightarrow F \subseteq G$$

$F \preceq G$ e' per costruzione algebrica

$$f(x) \in G[x], f(\alpha) = 0 \Rightarrow \alpha \text{ algebrico in } G \xRightarrow{[2.43,pg.31]} G \preceq G(\alpha) \text{ algebrica}$$

$$F \preceq G \preceq G(\alpha) \xRightarrow{[2.45,pg.31]} F \preceq G(\alpha) \text{ algebrica} \Rightarrow \alpha \text{ algebrico su } F \Rightarrow \alpha \in G$$

In definitiva, preso un $f(x) \in G[x]$ troviamo $\alpha \in G : f(\alpha) = 0$. Quindi G e' chiuso.

$$\begin{cases} G \text{ chiuso} \\ F \preceq G \text{ algebrica} \end{cases} \Rightarrow G = \overline{F}$$

□

Example 2.64.

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

Basta applicare la prop [2.63,pg.49] considerando l'estensione $\mathbb{Q} \preceq \mathbb{C}$, e il thm [6.39,pg.109].

3 Campi finiti

Definition 3.1. Un campo F e' finito $\stackrel{\text{def}}{\Leftrightarrow} |F| < \infty$

Proposition 3.2. Sia $F \preceq K$ una estensione, $p, n \in \mathbb{N}$, allora

$$\begin{cases} |F| = p \\ \dim_F K = n \end{cases} \Rightarrow |K| = p^n$$

Proof:

F^n e' uno spazio vettoriale su F

$$\dim_F K = n = \dim_F F^n \xRightarrow{[AL,7.6,pg.40]} K_F \simeq F^n \Rightarrow |K_F| = |F^n| = |F|^n = p^n$$

□

Proposition 3.3.

$$K \text{ campo finito} \Rightarrow \begin{cases} \text{ch} K = p \\ |K| = p^n, \text{ } p \text{ primo}, n \in \mathbb{N}^* \end{cases}$$

Non vale il viceversa:

$$\text{ch} K = p \not\Rightarrow K \text{ finito}$$

Proof:

(1) Dim. $\Rightarrow$

$$K \text{ campo} \Rightarrow \text{ch}K = 0 \vee \text{ch}K = p \quad (1)$$

$$\text{ch}K = 0 \xRightarrow{\substack{[2.11, \text{pg.} 13]}} \mathbb{Q} \hookrightarrow K \text{ assurdo contro } K \text{ finito}$$

$$\text{ch}K \neq 0 \xRightarrow{(1)} \text{ch}K = p \xRightarrow{\substack{[2.11, \text{pg.} 13]}} \mathbb{Z}_p \preceq K$$

$$K \text{ finito} \Rightarrow n = \dim_{\mathbb{Z}_p} K < \infty$$

$$\begin{cases} |\mathbb{Z}_p| = p \\ \mathbb{Z}_p \subseteq K \text{ estensione finita, } \dim_{\mathbb{Z}_p} K = n \end{cases} \xRightarrow{\substack{[3.2, \text{pg.} 50]}} |K| = p^n$$

(2) $\text{Dim} \neq$

$$\begin{aligned} & \mathbb{Z}_p(x), \quad \text{con } x \text{ indeterminata, o elemento trascendente su } \mathbb{Z}_p \\ & |\mathbb{Z}_p(x)| \xRightarrow{\substack{\geq \\ \text{vedi } [2.21, \text{pg.} 18]}} |\mathbb{Z}_p[x]| = \infty \end{aligned}$$

$$\text{ch}\mathbb{Z}_p(x) \xRightarrow{\substack{[2.8, \text{pg.} 12]}} \text{ch}\mathbb{Z}_p = p$$

Abbiamo così trovato un campo infinito con caratteristica p .

□

Proposition 3.4. *Sia K campo.*

$$|K| = p^n, \quad p \text{ primo} \Rightarrow K = CS(x^{p^n} - x, \mathbb{Z}_p) = \{\alpha \mid \alpha^{p^n} - \alpha = 0\}$$

Proof: Sia $f(x) = x^{p^n} - x \in \mathbb{Z}_p$. Consideriamo il gruppo moltiplicativo $(K^*, \cdot)$
 $|K^*| = p^n - 1$

$$\alpha \in K^* \xRightarrow{\substack{[AII, 1.57, \text{pg.} 21]}} \alpha^{|K^*|} = 1 \Leftrightarrow \alpha^{p^n-1} = 1 \Leftrightarrow \alpha^{p^n} = \alpha \Leftrightarrow f(\alpha) = 0$$

$$\forall \alpha \in K^* \quad f(\alpha) = 0 \quad (1)$$

$$f(0) = 0$$

$$\Rightarrow K = \{\alpha_i \mid f(\alpha_i) = 0 \quad \forall i = 1, \dots, \deg f(x) = p^n\} \quad (2)$$

$$(1) \xRightarrow{\substack{\text{Ruffini}}} x - \alpha \mid f(x) \quad \forall \alpha \in K^* \quad (3)$$

$$\deg f(x) = p^n \xRightarrow{(3)} f(x) = \prod_{i=1}^{p^n} (x - \alpha_i) \quad (4)$$

$$|K| = p^n < \infty \xRightarrow{\substack{[3.3, \text{pg.} 50]}} \text{ch}K = p \xRightarrow{\substack{[2.11, \text{pg.} 13]}} \mathbb{Z}_p \subseteq K \xRightarrow{(2)} K = \mathbb{Z}_p(\alpha_1, \dots, \alpha_{p^n}) \quad (2.2)$$

$$(2.2), (4) \Rightarrow K = CS(f(x), \mathbb{Z}_p)$$

□

Corollary 3.5. *Siano K, K' campi, allora*

$$|K| = |K'| < \infty \Rightarrow K \simeq K'$$

Proof:

$$\begin{aligned}
|K| = |K'| < \infty &\xRightarrow{[3.3, \text{pg.} 50]} |K| = |K'| = p^n \\
|K| = p^n, |K'| = p^n &\xRightarrow{[3.4, \text{pg.} 51]} K = CS(x^{p^n} - x, \mathbb{Z}_p) = K' \xRightarrow{[2.53, \text{pg.} 41]} K \simeq K'
\end{aligned}$$

□

Proposition 3.6. Sia $p, n \in \mathbb{N}^*$, p primo. Sia $f(x) \in \mathbb{Z}_p[x]$, $n = \deg f(x)$

$$f(x) \text{ irriducibile in } \mathbb{Z}_p \Rightarrow \begin{cases} \frac{\mathbb{Z}_p[x]}{(f(x))} \simeq \mathbb{Z}_p(\alpha) & \text{e' un campo} \\ |\mathbb{Z}_p(\alpha)| = p^n \\ \dim_{\mathbb{Z}_p} \mathbb{Z}_p(\alpha) = n \end{cases}$$

dove α e' una radice di $f(x)$. Nota: questa proposizione non garantisce l'esistenza di un campo K con p^n elementi, perche' a priori potrebbero non esistere $f(x)$ irriducibili in $\mathbb{Z}_p[x]$, di grado n .

Proof: Poiche' $n > 0$, possiamo considerare $f(x) = ag(x)$, $a, g(x) \in \mathbb{Z}_p[x]$, $g(x)$ monico. $f(x)$ irriducibile in $\mathbb{Z}_p \Rightarrow g(x)$ irriducibile in $\mathbb{Z}_p$

Per la prop [2.48, pg. 34] $\exists \alpha : g(\alpha) = 0$

$$\begin{cases} g(x) \text{ irriducibile in } \mathbb{Z}_p \\ g(\alpha) = 0 \\ g(x) \text{ monico} \end{cases} \xRightarrow{[2.30, \text{pg.} 24]} g(x) = P_{\min}(\alpha, \mathbb{Z}_p), \quad \frac{\mathbb{Z}_p[x]}{(g(x))} \simeq \mathbb{Z}_p[\alpha] \xRightarrow{[2.37, \text{pg.} 27]} \mathbb{Z}_p(\alpha) \quad \text{che e' un campo}$$

Osserviamo che $(f(x)) = (ag(x)) = (g(x))$. Infine,

$$g(x) = P_{\min}(\alpha, \mathbb{Z}_p), \quad \deg g(x) = \deg f(x) = n \Rightarrow$$

$$\xRightarrow{[2.40, \text{pg.} 29]} \mathbb{Z}_p(\alpha) = \mathcal{L}(1, \alpha, \dots, \alpha^{n-1})_{\mathbb{Z}_p} = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}_p\}$$

Quindi, poiche' ogni a_i puo' assumere p diversi valori, si ha

$$|\mathbb{Z}_p(\alpha)| = p^n$$

□

Proposition 3.7. Sia $p, n \in \mathbb{N}^*$, p primo. Si ha

$$\exists K \text{ campo: } |K| = p^n$$

In particolare, usando la prop [3.6, pg. 52], se $f(x) \in \mathbb{Z}_p[x]$ e' irriducibile, con $\deg f(x) = n$, un tale K sara'

$$K = \mathbb{Z}_p(\alpha), \quad \text{con } f(\alpha) = 0$$

Proof: Sia

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$$

$$L = CS(f(x), \mathbb{Z}_p)$$

$$K = \{\alpha \in L \mid f(\alpha) = 0\}$$

(1) $|K| = p^n$

Consideriamo il derivato di $f(x)$ (vedi [1.14, pg. 4]) per controllare le radici multiple di $f(x)$:

$$f'(x) = p^n x^{p^n-1} - 1 \xRightarrow{\text{siamo in } \mathbb{Z}_p: p=0} -1$$

$$f'(x) = -1 \neq 0 \quad \forall x \in \mathbb{Z}_p \xRightarrow{[1.17, \text{pg.} 6]} \mu_f(\alpha) = 1 \quad \forall \alpha \in K$$

$$\Rightarrow \text{tutte le } p^n \text{ radici di } f(x) \text{ sono distinte} \Rightarrow |K| = p^n$$

(2) K e' un campo

Dimostriamo che $K \preceq L$. Per la prop [1.6,pg.1], bastera' dimostrare che

$$(K, +) \leq (L, +), \quad (K^*, \cdot) \leq (L^*, \cdot)$$

(2.1) $(K, +) \leq (L, +)$

Poiche' K e' finito, per la prop [AII,1.22,pg.8], basta dimostrare che

$$\forall a, b \in K \quad a + b \in K$$

Si ha

$$a, b \in K \Rightarrow f(a) = f(b) = 0 \Leftrightarrow a^{p^n} - a = b^{p^n} - b = 0 \Leftrightarrow \begin{cases} a^{p^n} = a \\ b^{p^n} = b \end{cases} \quad (1)$$

$$(a + b)^p \underset{\substack{= \\ [1.20, \text{pg.7}]}}{=} a^p + b^p$$

$$(a + b)^{p^2} = ((a + b)^p)^p = (a^p + b^p)^p \underset{\substack{= \\ [1.20, \text{pg.7}]}}{=} a^{p^2} + b^{p^2}$$

$\vdots$

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \underset{(1)}{=} a + b$$

$$(a + b)^{p^n} - (a + b) = 0 \Rightarrow f(a + b) = 0 \Rightarrow a + b \in K$$

(2.2) $(K^*, \cdot) \leq (L^*, \cdot)$

Poiche' K^* e' finito, per la prop [AII,1.22,pg.8], basta dimostrare che

$$\forall a, b \in K^* \quad ab \in K^*$$

Si ha

$$(ab)^{p^n} \underset{\substack{= \\ L \text{ e' commutativo}}}{=} a^{p^n} b^{p^n} \underset{(1)}{=} ab$$

$$(ab)^{p^n} - ab = 0 \Leftrightarrow f(ab) = 0 \Rightarrow ab \in K^*$$

□

Proposition 3.8. *Sia K campo,*

$$|K| < \infty \Rightarrow (K^*, \cdot) \text{ e' un gruppo ciclico}$$

Proof: Sia $m = \text{mcm} \{o(a) \mid a \in K^*\}$. Sia $h = |K^*|$. Consideriamo $g(x) = x^m - 1$.

Per costruzione $\forall a \in K^* \exists \lambda_a : m = \lambda_a o(a)$

$$a^m = a^{\lambda_a o(a)} = 1$$

$$g(a) = a^m - 1 = 0 \quad \forall a \in K^* \quad \Rightarrow \quad h \leq \deg g(x) = m \quad (1)$$

[AI,16.1,pg.66]

$$a^h \underset{\substack{= \\ [AII,1.57, \text{pg.21}]}{=} 1 \quad \forall a \in K^* \Rightarrow o(a) \mid h \quad \forall a \in K^* \Rightarrow m \mid h \Rightarrow m \leq h \quad (2)$$

$$(1), (2) \Rightarrow h = m$$

$$\begin{cases} (K^*, \cdot) \text{ abeliano} \\ m = \text{mcm} \{o(a) \mid a \in K^*\} \end{cases} \underset{\substack{= \\ [AII,4.3, \text{pg.96}]}{=} \quad \exists c \in K^* : o(c) = m = h = |K^*| \Rightarrow K^* = \langle c \rangle$$

□

Proposition 3.9. *Sia p primo*

$$\forall n \in \mathbb{N}, n \geq 2 \quad \exists f(x) \in \mathbb{Z}_p[x] \text{ irriducibile, } \deg f(x) = n$$

Proof: Per la prop [3.7,pg.52],

$$p \text{ primo, } n \in \mathbb{N} \quad \underbrace{\Rightarrow}_{[3.7,pg.52]} \quad \exists K \text{ campo: } |K| = p^n \quad \underbrace{\Rightarrow}_{[3.4,pg.51]} \quad K = CS \left(x^{p^n} - x, \mathbb{Z}_p \right) \quad (1)$$

$$\begin{cases} |\mathbb{Z}_p| = p \\ (1) \Rightarrow \mathbb{Z}_p \preceq K \\ m = [K : \mathbb{Z}_p] \end{cases} \quad \underbrace{\Rightarrow}_{[3.2,pg.50]} \quad |K| = p^m \quad \underbrace{=}_{(1)} p^n \quad \underbrace{\Rightarrow}_{p>1} n = m = [K : \mathbb{Z}_p] \quad (2)$$

$$\begin{cases} \mathbb{Z}_p \text{ finito} \\ (1) \Rightarrow \mathbb{Z}_p \preceq K \text{ algebrica} \end{cases} \quad \underbrace{\Rightarrow}_{[3.27,pg.62]} \quad \mathbb{Z}_p \preceq K \text{ separabile} \quad (3)$$

$$\mathbb{Z}_p \preceq K \text{ finita} \quad \underbrace{\Rightarrow}_{[2.44,pg.31]} \quad \mathbb{Z}_p \preceq K \text{ finitamente generata} \quad (4)$$

$$(3), (4) \quad \underbrace{\Rightarrow}_{[3.29,pg.65]} \quad K = \mathbb{Z}_p(\alpha)$$

$$\underbrace{n}_{(2)} = [K : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] \quad \underbrace{=}_{[2.40,pg.29]} \quad \deg P_{\min}(\alpha, \mathbb{Z}_p)$$

$$\deg P_{\min}(\alpha, \mathbb{Z}_p) = n$$

E poiche' il polinomio minimo e' irriducibile, abbiamo la tesi. $\square$

Proposition 3.10. *I campi finiti si possono costruire concretamente. Per costruire il campo K con $|K| = q = p^n$, allora procediamo cosi':*

1. Cerchiamo $f(x)$ polinomio irriducibile monico in $\mathbb{Z}_p[x]$, con $\deg f(x) = n$. Tale $f(x)$ esiste per la [3.9,pg.54].
Per trovarlo si puo' procedere per forza bruta perche' $|\mathbb{Z}_p[x]| < \infty$
2. Allora, per la [3.6,pg.52] possiamo porre:

$$K = \mathbb{Z}_p(\alpha) = \mathbb{Z}_p[\alpha] \quad \underbrace{=}_{[2.35,pg.26]} \quad \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Z}_p\} \quad (*)$$

3. Infine, per la (*) possiamo rappresentare K come lo spazio vettoriale dei polinomi con grado $\leq n-1$:

$$K \simeq \mathbb{Z}_p[x]_{n-1}$$

e in particolar modo come lo spazio vettoriale $\mathbb{Z}_p^n$.

Quindi, K diventa semplicemente un insieme di n -uple di $\mathbb{Z}_p$. (nota¹⁵)

¹⁵chiaramente il prodotto tra due tuple e' il prodotto polinomiale con resto, ovvero

$$\begin{aligned} c &= (c_0, \dots, c_{n-1}), \quad d = (d_0, \dots, d_{n-1}) \\ c(x) &= c_0 + c_1x + \dots + c_{n-1}x^{n-1}, \quad d(x) = d_0 + d_1x + \dots + d_{n-1}x^{n-1} \\ cd &= (\text{i coefficienti di } c(\alpha)d(\alpha)) \end{aligned}$$

3.1 Proprieta' di $x^{p^n} - x$

Proposition 3.11. *Sia p un primo,*

$$f(x) \in \mathbb{Z}_p[x] \text{ monico, irriducibile, } \deg f = n \Rightarrow f(x) \Big/ x^{p^n} - x$$

Proof: Sia $g(x) = x^{p^n} - x$.

Sia $\alpha \in CS(f(x), \mathbb{Z}_p)$ una radice di $f(x)$.

$$f(x) \in \mathbb{Z}_p[x] \text{ irrid.} \quad \underbrace{\Rightarrow}_{[3.6, \text{pg.52}]} |\mathbb{Z}_p(\alpha)| = p^n \quad \underbrace{\Rightarrow}_{[3.4, \text{pg.51}]} \mathbb{Z}_p(\alpha) = \left\{ \beta \mid \beta^{p^n} - \beta = 0 \right\} \Rightarrow g(\alpha) = \alpha^{p^n} - \alpha = 0 \quad (1)$$

$$\begin{cases} f(x) \in \mathbb{Z}_p[x] \text{ monico, irriducibile} \\ f(\beta) = 0 \end{cases} \quad \underbrace{\Rightarrow}_{[2.30, \text{pg.24}]} f(x) = P_{\min}(\alpha, \mathbb{Z}_p) \quad (2)$$

$$(1), (2) \quad \underbrace{\Rightarrow}_{[2.28, \text{pg.23}]} f(x) \Big/ g(x)$$

□

Proposition 3.12.

$$x^{p^n} - x \text{ e' separabile}$$

Proof: Sia K un campo di p^n elementi (esiste per la [3.7, pg.52]). Sia $g(x) = x^{p^n} - x$

$$|K| = p^n \quad \underbrace{\Rightarrow}_{[3.4, \text{pg.51}]} p^n = |K| = |CS(g(x), \mathbb{Z}_p)| \quad \underbrace{=}_{[3.4, \text{pg.51}]} |\{\alpha \mid g(\alpha) = 0\}| \Rightarrow |\{\alpha \mid g(\alpha) = 0\}| = p^n = \deg g(x) \Rightarrow g(x) \text{ e'}$$

□

Lemma 3.13.

$$d \Big/ n \Rightarrow x^{p^d} - x \Big/ x^{p^n} - x$$

Proof: Vale la seguente proprieta':

$$a \Big/ b \Rightarrow (x^a - 1) \Big/ (x^b - 1) \quad (1)$$

infatti

$$\begin{aligned} a \Big/ b &\Rightarrow b = am \\ x^b - 1 &= x^{am} - 1 = (x^a - 1)(x^{a(m-1)} + x^{a(m-2)} + \dots + 1) \end{aligned}$$

Quindi

$$d \Big/ n \Rightarrow \underbrace{\Rightarrow}_{(1)} (p^d - 1) \Big/ (p^n - 1) \underbrace{\Rightarrow}_{(1)} x^{p^d-1} - 1 \Big/ x^{p^n-1} - 1 \quad \underbrace{\Leftrightarrow}_{\text{moltiplicando per } x} x^{p^d} - x \Big/ x^{p^n} - x$$

□

Theorem 3.14. *Sia p primo e sia*

$$x^{p^n} - x = f_1(x)f_2(x) \cdots f_h(x), \quad \text{con } f_i(x) \in \mathbb{Z}_p[x] \text{ monico, irriducibile } \forall i$$

la decomposizione in fattori irriducibili di $x^{p^n} - x$, allora

$$\{f_i(x) \mid i = 1, \dots, h\} = \left\{ f(x) \mid f(x) \in \mathbb{Z}_p[x] \text{ irriducibile, monico, } \deg f(x) \Big/ n \right\}$$

Inoltre, i due insiemi hanno cardinalita' h .

Proof: Sia A il primo insieme e B il secondo.

Sia $g(x) = x^{p^n} - x$. Sia

$$K = CS(x^{p^n} - x, \mathbb{Z}_p) \underset{[3.4, \text{pg.51}]}{=} \left\{ \alpha \mid \alpha^{p^n} - \alpha = 0 \right\}$$

(1) Dim. $A \subseteq B$

$$f_i(x) \nmid g(x) = \prod_{\alpha \in K} x - \alpha \Rightarrow \exists \alpha \in K : f_i(\alpha) = g(\alpha) = 0$$

$$f_i \text{ irrid.}, f_i(\alpha) = 0 \underset{[3.6, \text{pg.52}]}{\Rightarrow} [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = d = \deg f(x)$$

$$\mathbb{Z}_p \preceq \mathbb{Z}_p(\alpha) \underset{\alpha \in K}{\preceq} K \underset{[2.18, \text{pg.16}]}{\Rightarrow} d \mid [K : \mathbb{Z}_p] = n \Rightarrow f_i(x) \in B$$

(2) $B \subseteq A$

Sia $f(x) \in B$, $\deg f = d$,

$$f(x) \text{ monico, irriducibile}, \deg f = d \underset{[3.11, \text{pg.55}]}{\Rightarrow} f(x) \nmid x^{p^d} - x \underset{[3.13, \text{pg.55}]}{\nmid} x^{p^n} - x$$

$$f(x) \nmid g(x), f(x) \text{ monico, irrid.} \Rightarrow f(x) \in A$$

(3) $|A| = |B| = h$

Per la [3.12, pg.55] sappiamo che $g(x)$ e' separabile. Se per assurdo $\exists i \neq j : f_i(x) = f_j(x)$ allora

$$f_i(x)f_j(x) = f_i(x)^2 \nmid g(x) \underset{f_i(x) \text{ fattore irrid di } g(x)}{\Rightarrow} \exists \alpha : f_i(\alpha) = f_i(\alpha)^2 = g(\alpha) = 0 \Rightarrow \mu_g(\alpha) \geq 2$$

assurdo contro $g(x)$ separabile

Quindi $|A| = h$.

□

Corollary 3.15.

$$\sum_{d: d \mid n} d \left| \{ f(x) \in \mathbb{Z}_p[x], \text{ monico, irrid, } \deg f = d \} \right| = p^n$$

Proof: Utilizziamo il thm [3.14, pg.55],

$$\begin{aligned} p^n = \deg(x^{p^n} - x) &= \deg(f_1(x) \dots f_h(x)) = \sum_{i=1}^h \deg f_i \underset{[3.14, \text{pg.55}]}{=} \sum_{f(x) \in \mathbb{Z}_p[x] \text{ irrid, monico, } d=\deg f(x)} d = \\ &= \sum_{d: d \mid n} \sum_{f(x) \in \mathbb{Z}_p[x] \text{ irrid, monico, } \deg f(x)=d} d = \sum_{d: d \mid n} \left| \{ f(x) \in \mathbb{Z}_p[x], \text{ monico, irrid, } \deg f = d \} \right| \end{aligned}$$

□

Proposition 3.16. *Posto*

$$\begin{aligned} G_d &= \{ f(x) \in \mathbb{Z}_p[x], \text{ monico, irrid, } \deg f = d \} \\ g_d &= |G_d| \end{aligned}$$

si ha

$$g_n = \frac{p^n - \sum_{d/n, d < n} dg_d}{n}$$

In particolare,

$$|\{f(x) \in \mathbb{Z}_p[x] \text{ irrid, deg } f = n\}| = (p-1)g_n$$

Proof: Utilizzando il cor [3.15,pg.56]:

$$p^n \underbrace{=}_{[3.15,pg.56]} \sum_{d: d/n} dg_d = \sum_{d: d/n, d < n} dg_d + ng_n \Rightarrow g_n = \frac{p^n - \sum_{d: d/n, d < n} dg_d}{n}$$

Infine,

$$|\{f(x) \in \mathbb{Z}_p[x] \text{ irrid, deg } f = n\}| = |\{(\lambda, f(x)) \mid \lambda \in \mathbb{Z}_p^*, f(x) \in \mathbb{Z}_p[x] \text{ monico, irrid., deg } f = n\}| = |\mathbb{Z}_p^*|g_n = (p-1)g_n$$

□

Proposition 3.17. Siano F, K due campi con $|F| = p^d$, $|K| = p^n$

$$d/n \Leftrightarrow F \hookrightarrow K$$

Di conseguenza, e' sempre possibile scrivere una estensione $F \subseteq K$ di campi finiti con caratteristica p , come

$$\begin{aligned} F_{p^n} &\subseteq F_{p^{mn}} \\ F_q &\subseteq F_{q^m} \\ \text{con } q &= p^n, \quad F_q = F, \quad F_{q^m} = K \end{aligned}$$

dove F_q indica un campo di cardinalita' q (nota¹⁶).

Proof:

(1) Dim. $\Rightarrow$

$$\begin{aligned} d/n &\underbrace{\Rightarrow}_{[3.13,pg.55]} x^{p^d} - x / x^{p^n} - x \quad (1) \\ |F| = p^d &\underbrace{\Rightarrow}_{[3.4,pg.51]} F \simeq \left\{ \alpha \mid \alpha^{p^d} - \alpha = 0 \right\} \underbrace{\subseteq}_{(1)} \left\{ \alpha \mid \alpha^{p^n} - \alpha = 0 \right\} \underbrace{\simeq}_{[3.4,pg.51]} K \end{aligned}$$

(2) Dim. $\Leftarrow$

Per la prop [3.2,pg.50] si ha

$$p^n = |K| \underbrace{=}_{[3.2,pg.50]} (p^d)^{[K:F]} = p^{d[K:F]} \Rightarrow n = d[K:F] \Rightarrow d/n$$

□

¹⁶Per la [3.5,pg.51], tutti i campi di cardinalita' finita e fissata sono isomorfi. Quindi F_q puo' indicare uno qualsiasi dei campi di cardinalita' q

3.2 Estensioni separabili

Definition 3.18. Sia F campo, $f(x) \in F[x]$, $\deg f(x) = n$, $\alpha_1, \dots, \alpha_n \in CS(f(x), F[x])$ le radici di $f(x)$. Poniamo

$$f(x) \text{ e' separabile} \stackrel{\text{def}}{\Leftrightarrow} \alpha_i \neq \alpha_j \quad \forall i \neq j$$

In altre parole, $f(x)$ e' separabile se tutte le sue radici sono distinte. O equivalentemente, se $f(x)$ non ha radici multiple.

Sia $F \preceq K$ una estensione, $\alpha \in K$. Poniamo

$$\alpha \text{ e' separabile in } F \stackrel{\text{def}}{\Leftrightarrow} \alpha \text{ e' algebrico su } F, \quad P_{\min}(\alpha, F) \text{ e' separabile}$$

$$F \preceq K \text{ e' una estensione separabile} \stackrel{\text{def}}{\Leftrightarrow} F \preceq K \text{ e' algebrica, } \forall \alpha \in K \quad \alpha \text{ e' separabile}$$

Proposition 3.19. Sia $F[x]$ campo, $f(x), g(x) \in F[x]$, si ha

$$\begin{cases} f(x) \text{ separabile} \\ g(x)/f(x) \end{cases} \Rightarrow g(x) \text{ separabile}$$

Proof:

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

$$f(x) \text{ separabile} \Rightarrow \alpha_i \neq \alpha_j \quad \forall i \neq j \quad (1)$$

$$g(x)/f(x) \Rightarrow \exists i_1, \dots, i_r : \quad g(x) = \prod_{j=1}^r (x - \alpha_{i_j}) \underbrace{\Rightarrow}_{(1)} g(x) \text{ separabile}$$

□

Proposition 3.20. Sia $F \preceq K$ una estensione, $f(x), g(x) \in F[x]$. Siano inoltre

$$d_1(x) = \text{MCD}(f(x), g(x)) \in F[x] \text{ il massimo comune divisore in } F[x], \text{ ovvero}$$

$$d_1(x)/f(x), d_2(x)/g(x) \text{ in } F[x], \text{ ovvero}$$

$$\begin{cases} f(x) = \lambda(x)d_1(x), \quad \lambda(x), d_1(x) \in F[x] \\ g(x) = \mu(x)d_2(x), \quad \mu(x) \in F[x] \end{cases}$$

$$d_2(x) = \text{MCD}(f(x), g(x)) \in K[x]$$

allora

$$d_1(x) = d_2(x)$$

In pratica, il MCD non varia all'interno di una estensione.

Proof: Basta osservare che nei domini euclidei vale l'algoritmo di divisione. Quindi, possiamo usare l'algoritmo euclideo per il calcolo del MCD.

Le operazioni eseguite dall'algoritmo rimangono tutte in $F[x]$ (sono tutte divisioni con resto). Quindi, anche quando calcoliamo il MCD in $K[x]$, in realta' non stiamo mai uscendo da $F[x]$. □

Proposition 3.21. *Sia F campo,*

$$\begin{cases} g(x) \in F[x] \text{ e' irriducibile} \\ g'(x) \neq 0 \end{cases} \Rightarrow g(x) \text{ e' separabile}$$

dove con $g'(x)$ indichiamo la derivata di $g(x)$ (vedi [1.14,pg.4]).

Proof: Sia $K = CS(g(x), F)$. Supponiamo per assurdo che $g(x)$ abbia una radice multipla $\alpha \in K$. Sia

$$\begin{aligned} g'(x) &\text{ il derivato di } g(x) \\ d(x) &= \text{MCD}(g(x), g'(x)) \in F[x] \end{aligned}$$

Si ha

$$\alpha \text{ radice multipla} \Rightarrow \mu(\alpha) > 1 \xRightarrow{\text{[1.17,pg.6]}} g'(\alpha) = 0$$

$$g(\alpha) = 0, \quad g'(\alpha) = 0 \Rightarrow (x - \alpha) \mid g(x), \quad (x - \alpha) \mid g'(x) \xRightarrow{(*)} (x - \alpha) \mid d(x) \Rightarrow \deg d(x) \geq 1 \quad (1)$$

(*) $x - \alpha \in K[x]$, quindi $x - \alpha$ divide il MCD calcolato in $K[x]$, che per la prop [3.20,pg.58] coincide con $d(x)$.

$$d(x) \mid g(x) \Rightarrow g(x) = d(x)\lambda(x), \quad \lambda(x) \in F[x] \Rightarrow$$

$$\xRightarrow{\substack{d(x) \text{ invertibile} \vee \lambda(x) \text{ invertibile} \\ g(x) \text{ irriducibile in } F[x]}} d(x) \text{ invertibile} \vee \lambda(x) \text{ invertibile} \Leftrightarrow d(x) \equiv c \vee \lambda(x) \equiv k \Rightarrow \deg d(x) = 0 \vee d(x) = \frac{1}{k}g(x) \Rightarrow$$

$$\xRightarrow{(1)} d(x) = \frac{1}{k}g(x) \quad (2)$$

$$d(x) \mid g'(x) \xRightarrow{(2)} \frac{1}{k}g(x) \mid g'(x) \Rightarrow \deg g(x) \leq \deg g'(x) \quad (2.1)$$

$$g'(x) \text{ derivata di } g(x) \xRightarrow{\text{[1.16,pg.6]}} g'(x) \equiv 0 \vee \deg g'(x) < \deg g(x) \Rightarrow$$

$$\xRightarrow{g'(x) \neq 0 \text{ per Hp}} \deg g'(x) < \deg g(x) \text{ assurdo contro (2.1)}$$

□

Proposition 3.22. *Sia F campo,*

$$\begin{cases} \text{ch}F = 0 \\ g(x) \in F[x] \text{ e' irriducibile} \end{cases} \Rightarrow g(x) \text{ e' separabile}$$

Proof: Sia $K = CS(g(x), F)$. Per la proposizione [3.21,pg.59], basta dimostrare che $g'(x) \neq 0$. Supponiamo per assurdo $g'(x) \equiv 0$.

$$n = \deg g(x)$$

$$g(x) \text{ irriducibile} \Rightarrow g(x) \neq 0, \quad n \geq 1$$

$$g(x) = \sum_{i=0}^n a_i x^i \Rightarrow g'(x) = \sum_{i=1}^n i a_i x^{i-1} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

$$g'(x) \equiv 0 \Leftrightarrow a_1 = 2a_2 = \cdots = n a_n = 0 \Leftrightarrow \begin{cases} a_1 = 0 \\ 2 = 0 \vee a_2 = 0 \\ \cdots \\ n = 0 \vee a_n = 0 \end{cases} \quad (1)$$

$$g(x) \neq 0 \Rightarrow \exists j : a_j \neq 0 \xRightarrow{(1)} j = 0 \Leftrightarrow \underbrace{1 + 1 + \cdots + 1}_{j\text{-volte}} = 0 \xRightarrow{[2.4,pg.11]} \text{ch} F \neq 0$$

assurdo contro ipotesi.

□

Proposition 3.23. *Sia F campo.*

$$\begin{cases} \text{ch} F = 0 \\ F \preceq K \text{ estensione algebrica} \end{cases} \Rightarrow F \preceq K \text{ e' separabile}$$

Proof: Sia $\alpha \in K$

$$F \preceq K \text{ algebrica} \Rightarrow \alpha \text{ algebrico in } F \Rightarrow \exists f(x) = P_{\min}(\alpha, F)$$

$$f(x) = P_{\min}(\alpha, F) \xRightarrow{[2.30,pg.24]} f(x) \text{ irriducibile in } F \quad (1)$$

$$\begin{cases} \text{ch} F = 0 \\ (1) \end{cases} \xRightarrow{[3.22,pg.59]} f(x) \text{ e' separabile}$$

Quindi per definizione e per l'arbitrarietà di α , $F \preceq K$ e' separabile.

□

Proposition 3.24. *Sia F campo, $g(x) \in F[x]$, $n = \deg g(x)$. Si ha*

$$\begin{cases} \text{ch} F = p \\ g(x) \text{ irriducibile in } F[x] \\ p \nmid n \end{cases} \Rightarrow g(x) \text{ e' separabile}$$

Proof: Sia $K = CS(g(x), F)$. Per la proposizione [3.21,pg.59], basta dimostrare che $g'(x) \neq 0$.

Supponiamo per assurdo $g'(x) \equiv 0$.

$$g(x) \text{ irriducibile} \Rightarrow g(x) \neq 0, \quad n \geq 1$$

$$g(x) = \sum_{i=0}^n a_i x^i \Rightarrow g'(x) = \sum_{i=1}^n i a_i x^{i-1} = a_1 + 2a_2 x + \dots + n a_n x^{n-1}$$

$$g'(x) \equiv 0 \Leftrightarrow a_1 = 2a_2 = \dots = n a_n = 0 \Leftrightarrow \begin{cases} a_1 = \\ 2 = 0 \vee a_2 = 0 \\ \dots \\ n = 0 \vee a_n = 0 \end{cases} \quad (1)$$

$$\deg g(x) = n \Rightarrow a_n \neq 0 \underbrace{\Rightarrow}_{(1)} n = 0$$

$$\begin{cases} n \in \mathbb{N}^* \\ \text{ch} F = p \end{cases} \underbrace{\Rightarrow}_{[2.12, \text{pg.14}]} n \in \mathbb{Z}_p \underbrace{\Rightarrow}_{n=0} p/n$$

assurdo contro ipotesi.

□

Theorem 3.25. Sia F campo. $f(x) \in F[x]$ irriducibile. Si ha

$$f(x) \text{ e' non separabile} \Leftrightarrow \begin{cases} \text{ch} F = p \\ \exists g(x) \in F[x] : f(x) = g(x^p) \end{cases}$$

con p primo.

La condizione $f(x) = g(x^p)$, equivale a dire che $f(x)$ e' del tipo

$$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_n x^{np} = \sum_{i=0}^n a_i x^{ip}$$

Proof:

(1) Dim. $\Rightarrow$

Per Hp $f(x)$ e' irriducibile in $F[x]$ (1)

$$f(x) \text{ non separabile} \underbrace{\Rightarrow}_{[3.22, \text{pg.59}]} \text{ch} F \neq 0 \vee f(x) \text{ riducibile in } F \underbrace{\Rightarrow}_{(1)} \text{ch} F \neq 0 \Rightarrow$$

$$\underbrace{\Rightarrow}_{[2.7, \text{pg.12}]} \text{ch} F = p, \quad p \text{ primo}$$

$$f(x) \text{ non separabile} \underbrace{\Rightarrow}_{[3.21, \text{pg.59}]} f'(x) \equiv 0 \vee f(x) \text{ riducibile in } F \underbrace{\Rightarrow}_{(1)} f'(x) \equiv 0$$

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

$$f'(x) = a_1 + 2a_2 x + \dots + n a_n x^{n-1} \equiv 0 \Leftrightarrow i a_i = 0 \quad \forall i = 1, \dots, n \Leftrightarrow i = 0 \vee a_i = 0 \quad \forall i = 1, \dots, n \quad (2)$$

$$p \nmid i \Leftrightarrow i \neq 0 \underbrace{\Rightarrow}_{(2)} a_i = 0$$

$$a_i \neq 0 \Rightarrow p \mid i \Rightarrow i = \lambda_i p$$

Quindi gli unici coefficienti di $f(x)$ sono quelli del tipo $a_{\lambda_i p}$, perciò

$$f(x) = \sum_{i: a_i \neq 0} a_i x^i = \sum a_{\lambda_i p} x^{\lambda_i p} = \sum a_{\lambda_i p} (x^p)^{\lambda_i} = g(x^p)$$

$$\text{dove } g(x) = \sum a_{\lambda_i p} x^{\lambda_i}$$

(1) Dim. $\Leftarrow$

$$\text{ch}F = p \quad \underbrace{\Rightarrow}_{[2.12, \text{pg. } 14]} \quad p \in \mathbb{Z}_p$$

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

$$f'(x) = g'(x^p) p x^{p-1} \quad \underbrace{\equiv}_{p=0 \quad \mathbb{Z}_p} 0 \quad \underbrace{\Rightarrow}_{[1.17, \text{pg. } 6]} \quad \forall \alpha : f(\alpha) = 0 \quad \mu(\alpha) > 1$$

□

Corollary 3.26. *Sia F campo, $\text{ch}F = p$, p primo. Si ha*

$$f(x) \in F[x] \text{ irriducibile} \Rightarrow \exists g(x) \in F[x] \text{ irriducibile e separabile} : \exists e \in \mathbb{N} : f(x) = g(x^{p^e})$$

Proof: Costruiamo la seguente successione di polinomi: Se $f(x)$ e' separabile, basta porre $g(x) = f(x)$, $e = 0$.

Se $f(x)$ non e' separabile,

$$\begin{cases} f(x) \in F[x] \text{ irriducibile} \\ f(x) \text{ e' non separabile} \end{cases} \quad \underbrace{\Rightarrow}_{[3.25, \text{pg. } 61]} \quad \exists g_1(x) \in F[x] : f(x) = g_1(x^p)$$

$g_1(x)$ e' irriducibile, infatti, se per assurdo non lo fosse

$$g_1(x) = h(x)k(x) \Rightarrow f(x) = g_1(x^p) = h(x^p)k(x^p) \Rightarrow f(x) \text{ riducibile}$$

assurdo.

Se $g_1(x)$ e' separabile, abbiamo finito: $e = 1$.

Se $g_1(x)$ non e' separabile, allora

$$\begin{cases} g_1(x) \in F[x] \text{ irriducibile} \\ g_1(x) \text{ e' non separabile} \end{cases} \quad \underbrace{\Rightarrow}_{[3.25, \text{pg. } 61]} \quad \exists g_2(x) \in F[x] : g_1(x) = g_2(x^p)$$

e si ha

$$f(x) = g_1(x^p) \quad \underbrace{=}_{\text{ch}F=p, [1.20, \text{pg. } 7]} \quad g_1(x)^p = g_2(x^p)^p \quad \underbrace{=}_{\text{ch}F=p, [1.20, \text{pg. } 7]} \quad (g_2(x)^p)^p = g_2(x)^{p^2} = g_2(x^{p^2})$$

$$f(x) = g_2(x^{p^2})$$

Se $g_2(x)$ e' separabile, allora $e = 2$.

Così' continuando arriveremo a

$$f(x) = g_j(x^{p^j})$$

$$\deg f(x) \geq p^j$$

Se per assurdo, questo procedimento non dovesse avere fine, $f(x)$ avrebbe grado infinito. Assurdo. Quindi $\exists e : f(x) = g_e(x^{p^e})$, g_e separabile. □

Proposition 3.27. *Sia $F \preceq K$ una estensione*

$$\begin{cases} F \text{ campo finito} \\ F \preceq K \text{ algebrica} \end{cases} \quad \Rightarrow \quad F \preceq K \text{ e' separabile}$$

Proof: Sia $\alpha \in K$. Dobbiamo dimostrare che $f(x) = P_{\min}(\alpha, F)$ e' separabile.

$$F \preceq K \text{ algebrica} \Rightarrow \alpha \text{ algebrico su } F \Rightarrow \exists f(x) = P_{\min}(\alpha, F)$$

$$\text{Sia } n = \deg f(x)$$

$$\alpha \text{ algebrico su } F \xRightarrow{[2.40, \text{pg.29}]} \Rightarrow \dim_F F(\alpha) = n$$

$$\left\{ \begin{array}{l} F \preceq F(\alpha) \\ \dim_F F(\alpha) = n \\ |F| < \infty \end{array} \right. \xRightarrow{[3.2, \text{pg.50}]} |F(\alpha)| = |F|^n < \infty \xRightarrow{[3.3, \text{pg.50}]} \left\{ \begin{array}{l} \text{ch} F(\alpha) = p \\ |F(\alpha)| = p^n, p \text{ primo} \end{array} \right. \Rightarrow$$

$$\xRightarrow{[3.4, \text{pg.51}]} F(\alpha) = CS \left(\underbrace{x^{p^n} - x}_{g(x)}, \mathbb{Z}_p \right) = \{\beta \mid g(\beta) = 0\} \quad (1)$$

$$\alpha \in K \xRightarrow{(1)} g(\alpha) = 0 \xRightarrow{[2.28, \text{pg.23}]} g(x) \in (f(x)) \Rightarrow g(x) = \lambda(x)f(x) \quad (2)$$

$$\text{ch} F(\alpha) = p \xRightarrow{[2.12, \text{pg.14}]} p \in \mathbb{Z}_p$$

$$g'(x) = p^n x^{p^n-1} - 1 \underset{p=0 \text{ } \mathbb{Z}_p}{=} -1 \xRightarrow{[1.17, \text{pg.6}]} g(x) \text{ non ha radici multiple} \xRightarrow{(2)} f(x) \text{ non ha radici multiple}$$

□

Proposition 3.28. Sia $F \preceq K$ una estensione

$$F \preceq K \text{ separabile} \Rightarrow F \preceq K \text{ algebrica}$$

$$F \preceq K \text{ separabile} \not\Leftrightarrow F \preceq K \text{ algebrica}$$

Proof:

$$\langle 1 \rangle \text{ Dim.} \Rightarrow$$

Per definizione.

$$\langle 1 \rangle \text{ Dim} \not\Leftrightarrow$$

PROOF SKETCH: Portiamo un esempio di estensione $F \preceq K$ algebrica ma non separabile.

Per le prop [3.23,pg.60], [3.27,pg.62], F dovra' essere un campo infinito di caratteristica p .

Per dimostrare l'inseparabilita' di $F \preceq K$ dobbiamo trovare un $t \in K$: $P_{\min}(t, F)$ e' inseparabile.

Sia t un elemento trascendente su $\mathbb{Z}_p$. Sia $u = t^p$.

$$\langle 1.1 \rangle u \text{ e' trascendente su } \mathbb{Z}_p$$

Se per assurdo u fosse algebrico su $\mathbb{Z}_p$, allora $\exists f(x) \in \mathbb{Z}_p[x] : f(u) = 0 \Leftrightarrow f(t^p) = 0$.

$$f(x) = \sum_{i=0}^n a_i x^i$$

$$f(t^p) = \sum_{i=0}^n a_i (t^p)^i = \sum_{i=0}^n a_i (t)^{i+p} = g(t)$$

$$\text{dove } g(x) = \sum_{i=0}^n a_i x^{i+p} \in \mathbb{Z}_p[x]$$

$$g(t) = f(t^p) = 0 \Rightarrow t \text{ e' algebrico su } \mathbb{Z}_p$$

assurdo.

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

$u = t^p \in \mathbb{Z}_p(t) \Rightarrow \mathbb{Z}_p(u) \subseteq \mathbb{Z}_p(t) \Leftrightarrow F \preceq K$

$u = t^p \Rightarrow x^p - u \in F[x]$ ha t come radice $\Rightarrow t$ e' algebrico su $F \xRightarrow{[2.43, \text{pg.31}]} F \preceq F(t)$ algebrica (1)

$F(t) = \mathbb{Z}_p(u, t) \xRightarrow{u \in \mathbb{Z}_p(t)} \mathbb{Z}_p(t) = K$

$F(t) = K \xRightarrow{(1)} F \preceq K$ e' algebrica

Abbiamo cosi' trovato la nostra estensione algebrica $F \preceq K$. Resta da dimostrare la sua non separabilita'.

Consideriamo il polinomio $f(x) = x^p - u$

$u \in \mathbb{Z}_p(u) = F \Rightarrow f(x) \in F[x]$

(1.2) $f(x) = P_{\min}(t, F)$

Usiamo la caratterizzazione [2.30, pg.24]. Dimostriamo intanto l'irriducibilita'.

(1.2.1) $f(x)$ e' irriducibile in $F[x]$

Sia $F' = \mathbb{Z}_p[u]$

u trascendente in $\mathbb{Z}_p \xRightarrow{[2.34, \text{pg.26}]} \mathbb{Z}_p[u] \simeq \mathbb{Z}_p[x]$ (1)

$\mathbb{Z}_p$ UFD $\xRightarrow{\text{Gauss}[\text{AI}, 23.2, \text{pg.112}]} \mathbb{Z}_p[x]$ UFD $\xRightarrow{(1)} \mathbb{Z}_p[u]$ UFD $\Leftrightarrow F'$ UFD $\xRightarrow{\text{Gauss}[\text{AI}, 23.2, \text{pg.112}]} F'[x]$ UFD (2)

1, $u \in F' \Rightarrow f(x) = x^p - u \in F'[x]$

Possiamo allora cercare di applicare il Criterio di Eisenstein ([AI, 23.2, pg.113]).

(1.2.1.1) $u^2 \nmid u$ in F'

Se per assurdo $u^2 \mid u$ in $F' = \mathbb{Z}_p[u] \simeq \mathbb{Z}_p[x]$, allora,

$u^2 \mid u \Leftrightarrow \exists h(u) \in F' : u^2 h(u) = u \xRightarrow{F' \simeq \mathbb{Z}_p[x]} x^2 h(x) = x \Rightarrow 2 + \deg h(x) = 1 \Leftrightarrow \deg h(x) = -1$

assurdo.

(1.2.1.2) u e' primo in F'

$F' = \mathbb{Z}_p[u] \simeq \mathbb{Z}_p[x]$

x irriducibile in $\mathbb{Z}_p[x] \xLeftrightarrow{\mathbb{Z}_p[x] \text{ e' un ED, [1.8, pg.2]}} x \text{ primo in } \mathbb{Z}_p[x] \xLeftrightarrow{\mathbb{Z}_p[u] \simeq \mathbb{Z}_p[x]} u \text{ primo in } \mathbb{Z}_p[u]$

Notiamo che $f(x) = x^p - u$ e' primitivo ([AI, 16.2, pg.69]), in quanto x^p ha 1 come coeffi-

ciente.

$$\begin{array}{ccc}
 \left\{ \begin{array}{l} F' \text{ UFD} \\ f(x) \in F'[x] \\ f(x) = x^p - u \text{ primitivo} \\ u \text{ primo in } F' \\ u \not\mid u \\ u^2 \not\mid u \end{array} \right. & \xRightarrow{\text{Eisenstein [AI,23.2,pg.113]}} & f(x) \text{ e' irriducibile in } F'[x] \quad (3) \\
 (3) & \xRightarrow{\text{[AI,23.1,pg.112]}} & f(x) \text{ e' irriducibile in } Q(F')[x] = Q(\mathbb{Z}_p[u])[x] \xrightarrow{\simeq} \mathbb{Z}_p(u)[x] = F[x] \quad \text{[2.39,pg.28]}
 \end{array}$$

Nota¹⁷. Infine,

$$\begin{aligned}
 f(x) &\in F[x] \\
 f(t) &= t^p - u = t^p - t^p = 0 \\
 f(x) &\text{ e' monico} \\
 f(x) &\text{ e' irriducibile in } F[x]
 \end{aligned}$$

e quindi $f(x) = P_{\min}(t, F[x])$
 (1.3) Q.E.D.

$$\begin{aligned}
 &f(x) \in F[x] \subseteq K[x] \\
 \text{In } K[x], f(x) = x^p - u \text{ si puo' scrivere direttamente come} \\
 f(x) = \underbrace{x^p - t^p}_{\in K[x] = \mathbb{Z}_p(t)[x] \text{ [1.20,pg.7]}} &= \underbrace{(x - t)^p}_{= (x - t)^p} \Rightarrow f(x) \text{ ha una sola radice, che e' multipla} \Rightarrow \\
 &\Rightarrow f(x) \text{ non e' separabile}
 \end{aligned}$$

□

Theorem 3.29. Sia $F \preceq K$ una estensione,

$$F \preceq K \text{ finitamente generata, separabile} \Rightarrow F \preceq K \text{ e' semplice}$$

In particolare, si ha

$$\left\{ \begin{array}{l} F \text{ infinito} \\ K = F(\alpha, \beta), \quad \alpha, \beta \in K \Rightarrow K = F(\alpha + \lambda\beta) \quad \forall \lambda \in F : \lambda \neq \frac{\alpha - \alpha_i}{\beta_j - \beta} \quad \forall i = 1, \dots, n, \quad \forall j = 2, \dots, m \\ F \preceq K \text{ separabile} \end{array} \right.$$

dove $(\alpha = \alpha_1), \alpha_2, \dots, \alpha_n$ sono tutte le radici di $P_{\min}(\alpha, F)$

$(\beta = \beta_1), \beta_2, \dots, \beta_m$ sono tutte le radici di $P_{\min}(\beta, F)$

Proof:

$$F \preceq K \text{ fin. gen.} \Rightarrow \exists \alpha_1, \dots, \alpha_n \in K : K = F(\alpha_1, \dots, \alpha_n) \quad (1)$$

$$F \preceq K \text{ separabile} \Rightarrow F \preceq K \text{ algebrica} \quad (2)$$

CASE: F finito

¹⁷Non possiamo applicare direttamente Eisenstein in $\mathbb{Z}_p(u)$ perche' u non e' primo in $\mathbb{Z}_p(u)$ (e' infatti invertibile)

$$\begin{aligned}
(1), (2) & \xLeftrightarrow[2.44, \text{pg.} 31] F \preceq K \text{ finita} \\
& \left\{ \begin{array}{l} F \text{ finito} \\ F \preceq K \text{ finita} \end{array} \right. \xRightarrow[3.2, \text{pg.} 50]{} K \text{ finito} \xRightarrow[3.8, \text{pg.} 53]{} K^* \text{ e' ciclico} \Rightarrow \\
& \Rightarrow \exists \alpha \in K^* : K^* = \langle \alpha \rangle \Rightarrow K^* \subseteq F(\alpha) \xRightarrow[0 \in F(\alpha)]{} K \subseteq F(\alpha) \\
& \left\{ \begin{array}{l} F(\alpha) \subseteq K \text{ [per definizione]} \\ K \subseteq F(\alpha) \end{array} \right. \Rightarrow K = F(\alpha)
\end{aligned}$$

CASE: F infinito

Procediamo per induzione su n .

$\langle 0.1 \rangle \ n = 1$

$$(1) \Rightarrow K = F(\alpha_1)$$

quindi K e' semplice.

$\langle 0.2 \rangle \ n = 2$

$K = F(\alpha_1, \alpha_2)$. Chiamiamo $\alpha = \alpha_1$, $\beta = \alpha_2$, e quindi $K = F(\alpha, \beta)$.

$(2) \Rightarrow \exists f(x) = P_{\min}(\alpha, F)$, $\exists g(x) = P_{\min}(\beta, F)$

$F \preceq K$ separabile $\Rightarrow \alpha, \beta$ sono separabili $\Rightarrow P_{\min}(\alpha, F) = f(x)$, $P_{\min}(\beta, F) = g(x)$ sono separabili $\Rightarrow$

$$\Rightarrow \left\{ \begin{array}{l} \text{le } \{\alpha_1, \dots, \alpha_n\} \text{ sono tutte distinte (2.0)} \\ \text{le } \{\beta_1, \dots, \beta_n\} \text{ sono tutte distinte (2.1)} \end{array} \right.$$

Siano

$\alpha_1, \alpha_2, \dots, \alpha_n$ le radici di $f(x)$

$\beta_1, \beta_2, \dots, \beta_m$ le radici di $g(x)$

Sia $M = CS(f(x)g(x), F) = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$. Sia

$$\lambda_{ij} = \frac{\alpha - \alpha_i}{\beta_j - \beta} \in M \quad \forall i = 1, \dots, n, \quad \forall j = 2, \dots, m$$

Si ha

F infinito $\Rightarrow \exists \lambda \in F : \lambda \neq \lambda_{ij} \quad \forall i, j \Leftrightarrow (\beta_j - \beta)\lambda \neq \alpha - \alpha_i \Leftrightarrow \alpha + \beta\lambda \neq \alpha_i + \beta_j\lambda \quad \forall i, j \quad (3)$

Sia $\gamma = \alpha + \beta\lambda$

Sia $h(x) = f(\gamma - \lambda x)$

$\langle 0.2.1 \rangle \ \beta = \beta_1$ e' l'unico elemento di $\{\beta_1, \dots, \beta_m\}$ tale che $h(\beta) = 0$

β e' una radice di $h(x)$:

$$h(\beta) = f(\gamma - \lambda\beta) = f(\alpha + \beta\lambda - \lambda\beta) = f(\alpha) \xRightarrow[f(x)=P_{\min}(\alpha, F)]{} 0$$

Se β_j , con $j \neq 1$, fosse radice di $h(x)$:

$$f(\gamma - \lambda\beta_j) = 0 \Rightarrow \exists i : \alpha_i = \gamma - \lambda\beta_j \Leftrightarrow \alpha_i = \alpha + \beta\lambda - \lambda\beta_j \Leftrightarrow \alpha + \beta\lambda = \alpha_i + \beta_j\lambda$$

assurdo contro (3).

Poiche'

$$\gamma \in F(\gamma), \lambda \in F \Rightarrow h(x) = f(\gamma - \lambda x) \in F(\gamma)[x]$$

$$g(x) \in F[x] \subseteq F(\gamma)[x]$$

$$h(x), g(x) \in F(\gamma)[x]$$

per la prop. [3.20,pg.58], possiamo calcolare $d(x) = \text{MCD}(h(x), g(x))$ all'interno di $F(\gamma)[x]$.

$$g(x) = P_{\min}(\beta, F) \Rightarrow g(\beta) = 0 \Rightarrow x - \beta \mid g(x)$$

$$h(\beta) = 0 \Rightarrow x - \beta \mid h(x)$$

$$\Rightarrow x - \beta \mid d(x)$$

$$g(x) = (x - \beta)(x - \beta_2) \dots (x - \beta_m)$$

$$d(x) \mid g(x) \Rightarrow d(x) \text{ e' del tipo } (x - \beta_{j_1})(x - \beta_{j_2}) \dots (x - \beta_{j_s}) \quad (*)$$

$$(x - \beta_j) \mid d(x) \mid h(x) \Rightarrow h(\beta_j) = 0 \xRightarrow{\text{passo 0.2.1}} \beta_j = \beta$$

$$\xRightarrow{(2.1)} \beta \text{ e' l'unico t.c. } x - \beta \mid d(x) \xRightarrow{(*)} d(x) = x - \beta$$

$$\begin{cases} d(x) \in F(\gamma)[x] \\ d(x) = x - \beta \end{cases} \Rightarrow \beta \in F(\gamma)$$

$$\gamma = \alpha + \beta\lambda \Leftrightarrow \alpha = \gamma - \beta\lambda \quad \underbrace{\beta, \lambda}_{\in F \subseteq F(\gamma)} \in F(\gamma)$$

$$\alpha, \beta \in F(\gamma) \Rightarrow K = F(\alpha, \beta) \subseteq F(\gamma)$$

$$\alpha, \beta \in K = F(\alpha, \beta), \lambda \in F \subseteq K \Rightarrow \gamma \in K \Rightarrow F(\gamma) \subseteq K$$

$$\Rightarrow K = F(\gamma)$$

e quindi $F \preceq K$ e' semplice

(0.3) Passo induttivo: $P(n-1) \Rightarrow n$

$$(1) \Rightarrow K = F(\alpha_1, \dots, \alpha_n) \xRightarrow{[2.22, \text{pg.19}]} F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \xRightarrow{\text{Hp induttiva}} F(\beta)(\alpha_n) = F(\beta, \alpha_n) \xRightarrow{\text{passo 0.2}} F(\delta)$$

□

Example 3.30. Esempio di estensione finita, non separabile e non semplice.

Sia p primo, t, v trascendenti su $\mathbb{Z}_p$, $u = t^p$, $w = v^p$, $F = \mathbb{Z}_p(u, w)$, $K = \mathbb{Z}_p(t, v)$.

Si ha

$$F \subseteq K = F(t, v)$$

t, v sono algebrici su F , infatti, sono radice dei seguenti polinomi:

$$x^p - u, x^p - w \in F[x]$$

$$t, v \text{ algebrici su } F \xRightarrow{[2.43, \text{pg.31}]} F \preceq F(t, v) \text{ algebrica} \xRightarrow{[2.42, \text{pg.30}]} F \preceq F(t, v) \text{ finita}$$

Analogamente a quanto fatto nella dimostrazione [3.28,pg.63] (usando Eisenstein) si vede che

$$x^p - u = P_{\min}(t, F) \quad (1)$$

$$x^p - w = P_{\min}(v, F) \quad (1.1)$$

$$x^p - w \text{ e' irriducibile su } F(t) \quad (1.2)$$

Supponiamo per assurdo che $F \preceq K$ sia semplice, ovvero che $\exists \gamma \in K : K = F(\gamma)$.

$$\begin{aligned}
& F \subseteq F(t) \subseteq F(t, v) \\
(1) & \Rightarrow [F(t) : F] = p \\
(1.1) & \Rightarrow [F(t, v) : F(t)] \leq p \\
(1.2) & \Rightarrow \deg P_{\min}(v, F(t)) \geq p \Leftrightarrow [F(t, v) : F(t)] \geq p \\
& \Rightarrow [F(t, v) : F(t)] = p \\
& \begin{cases} [F(t) : F] = p \\ [F(t, v) : F(t)] = p \end{cases} \Rightarrow [F(t, v) : F] = p^2 \Leftrightarrow [K : F] = p^2 \quad (1)
\end{aligned}$$

Si ha

$$\begin{aligned}
\gamma \in K = F(t, v) & \Rightarrow \gamma = \frac{f(t, v)}{g(t, v)} = \frac{a_{00} + a_{01}v + a_{02}v^2 + \dots + a_{10}t + a_{11}tv + a_{21}t^2v + \dots}{b_{00} + b_{01}v + b_{02}v^2 + \dots + b_{10}t + b_{11}tv + b_{21}t^2v + \dots} \\
& \quad [2.21, \text{pg.18}] \\
\gamma^p & \stackrel{[1.20, \text{pg.7}]}{=} \frac{a_{00}^p + a_{01}^p v^p + a_{02}^p v^{2p} + \dots + a_{10}^p t^p + a_{11}^p t^p v^p + a_{21}^p t^{2p} v^p + \dots}{b_{00}^p + b_{01}^p v^p + b_{02}^p v^{2p} + \dots + b_{10}^p t^p + b_{11}^p t^p v^p + b_{21}^p t^{2p} v^p + \dots} = \\
& = \frac{a_{00}^p + a_{01}^p w + a_{02}^p w^2 + \dots + a_{10}^p u + a_{11}^p uw + a_{21}^p u^2 w + \dots}{b_{00}^p + b_{01}^p w + b_{02}^p w^2 + \dots + b_{10}^p u + b_{11}^p uw + b_{21}^p u^2 w + \dots} = \frac{\bar{f}(u, w)}{\bar{g}(u, w)} \in \mathbb{Z}_p(u, w) = F \Rightarrow \\
& \Rightarrow \gamma \text{ e' radice di } x^p - \frac{\bar{f}(u, w)}{\bar{g}(u, w)} \in F[x] \Rightarrow \deg P_{\min}(\gamma, F) \leq p \Rightarrow [F(\gamma) : F] \leq p \Leftrightarrow [K : F] \leq p
\end{aligned}$$

assurdo contro (1).

Quindi $F \preceq K$ non e' semplice. Inoltre, poiche' $F \preceq K = F(t, v)$ e' finitamente generata ma non semplice, per il thm [3.29, pg.65], possiamo dedurre che $F \preceq K$ non e' separabile.

Theorem 3.31. *Sia $F \preceq K$ una estensione finita, si ha*

$$F \preceq K \text{ e' semplice} \Leftrightarrow |\{L : F \prec L \prec K\}| < \infty$$

ovvero $F \preceq K$ e' semplice sse esiste un numero finito di campi strettamente compresi tra F e K .

Proposition 3.32.

$$\begin{cases} F \preceq L \text{ separabile} \\ F \preceq K \preceq L \end{cases} \Rightarrow \begin{cases} F \preceq K \\ K \preceq L \end{cases} \text{ separabili}$$

Proof: Sia $\alpha \in K$, $f(x) = P_{\min}(\alpha, F)$

$$\begin{cases} \alpha \in K \subseteq L \\ F \subseteq L \text{ separabile} \end{cases} \Rightarrow f(x) \text{ separabile}$$

Quindi $F \preceq K$ e' separabile.

Sia $\alpha \in L$, $f(x) = P_{\min}(\alpha, K)$, $g(x) = P_{\min}(\alpha, F)$

$$\begin{cases} f(x) = P_{\min}(\alpha, K), g(x) = P_{\min}(\alpha, F) \\ f(\alpha) = g(\alpha) = 0, g(x) \in F[x] \subseteq K[x] \end{cases} \Rightarrow f(x) \mid g(x) \quad (1)$$

$$F \preceq L \text{ separabile} \Rightarrow g(x) \text{ separabile} \quad (2)$$

$$(1), (2) \Rightarrow f(x) \text{ separabile}$$

[3.19, pg.58]

Quindi $K \preceq L$ e' separabile. □

Proposition 3.33.

$$\begin{cases} F \preceq F(\alpha_1, \dots, \alpha_n) \\ \alpha_i \text{ separabile su } F \quad \forall i = 1, \dots, n \end{cases} \Rightarrow F \preceq F(\alpha_1, \dots, \alpha_n) \text{ e' separabile}$$

Proof: Nota: faremo uso di teoremi che verranno dimostrati in seguito (ovviamente questi teoremi non fanno uso di questa stessa proposizione ;)

$$\begin{aligned} \alpha_i \text{ separabile } \forall i &\Rightarrow \begin{cases} \alpha_i \text{ algebrico su } F \\ p_i(x) = P_{\min}(\alpha_i, F) \text{ separabile} \end{cases} \quad \forall i \Rightarrow \\ &\underbrace{\Rightarrow}_{[2.43, \text{pg.31}]} F \subseteq F(\alpha_1, \dots, \alpha_n) \text{ e' algebrica e finitamente generata} \quad \underbrace{\Rightarrow}_{[2.44, \text{pg.31}]} F \subseteq K \text{ e' finita} \\ &\begin{cases} \alpha_1, \dots, \alpha_n \text{ sep. su } F \\ K = F(\alpha_1, \dots, \alpha_n) \\ F \subseteq K \text{ algebrica} \end{cases} \quad \underbrace{\Rightarrow}_{[6.18, \text{pg.90}]} \exists \gamma \in K \text{ separabile su } F \text{ t.c. } K = F(\gamma) \\ &\gamma \text{ separabile su } F \Rightarrow p(x) = P_{\min}(\gamma, F) \text{ e' separabile} \\ &\begin{cases} \text{Sia } J = CS(p(x), F) \\ p(x) \text{ separabile} \\ p(x) \in F[x] \end{cases} \quad \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} F \subseteq J \text{ e' di Galois} \Rightarrow F \subseteq J \text{ e' separabile} \\ &\begin{cases} p(\gamma) = 0 \Rightarrow \gamma \in J \\ F \subseteq J \end{cases} \Rightarrow F(\gamma) \subseteq J \Leftrightarrow K \subseteq J \\ &\begin{cases} F \subseteq K \subseteq J \\ F \subseteq J \text{ separabile} \end{cases} \quad \underbrace{\Rightarrow}_{[3.32, \text{pg.68}]} F \subseteq K \text{ separabile} \end{aligned}$$

□

4 Polinomi simmetrici

Definition 4.1. Sia F campo, $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$, ovvero

$$f(x_1, \dots, x_n) = \sum \alpha_{x_1, \dots, x_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

$x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ si chiama *monomio* di f . $\alpha_{x_1, \dots, x_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ si chiama *termine* di f .
Poniamo

$$\deg \alpha_{x_1, \dots, x_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \stackrel{\text{def}}{=} i_1 + i_2 + \dots + i_n$$

Dati i due monomi

$$\begin{aligned} a(x_1, \dots, x_n) &= x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \\ b(x_1, \dots, x_n) &= x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \end{aligned}$$

Definiamo il seguente ordinamento, chiamato *ordinamento lessicografico*:

$$a \leq b \stackrel{\text{def}}{\Leftrightarrow} \deg a < \deg b \vee \begin{cases} \deg a = \deg b \\ \exists t = \min \{t \mid i_t \neq j_t\} \Rightarrow i_t < j_t \end{cases}$$

Proposition 4.2. La relazione $\leq$ e' una relazione d'ordine totale sui termini di $F[x_1, \dots, x_n]$ e inoltre, posto

$$\begin{aligned}\underline{x} &= (x_1, \dots, x_n) \\ i &= (i_1, \dots, i_n) \in \mathbb{N}^n \\ j &= (j_1, \dots, j_n) \in \mathbb{N}^n \\ i + j &= (i_1 + j_1, \dots, i_n + j_n) \\ \underline{x}^i &= x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}\end{aligned}$$

si ha

1. $\underline{x}^i \leq \underline{x}^j \Rightarrow \underline{x}^{i+k} \leq \underline{x}^{j+k} \quad \forall k \in \mathbb{N}^n$
2. $\begin{cases} \underline{x}^i \leq \underline{x}^j \\ \underline{x}^h \leq \underline{x}^k \end{cases} \Rightarrow \underline{x}^{i+h} \leq \underline{x}^{j+k} \quad \forall k \in \mathbb{N}^n$
3. L'insieme $\{i \in \mathbb{N}^n \mid \underline{x}^i \leq \underline{x}^j\}$ e' finito

Proof: Intanto osserviamo che la relazione $\leq$ e' il realta' una relazione su $\mathbb{N}^n$, dove

$$i \leq j \Leftrightarrow i_1 + \dots + i_n < j_1 + \dots + j_n \vee \begin{cases} i_1 + \dots + i_n = j_1 + \dots + j_n \\ \exists t = \min \{t \mid i_t \neq j_t\} \Rightarrow i_t < j_t \end{cases}$$

Basta quindi ragionare sulle n -uple.

E' facile vedere che $(\mathbb{N}^n, \leq)$ e' una relazione d'ordine totale (e' in pratica quella del dizionario).

Infine, Se $i = j$, la 1. e' vera. Se $i \neq j$, per dimostrare la 1., basta osservare che

$$i \leq j \Rightarrow i_t < j_t \Rightarrow i_t + k_t < j_t + k_t$$

La 2. si ricava dalla 1.:

$$\begin{aligned}i \leq j &\Rightarrow i + h \leq j + h \\ h \leq k &\Rightarrow h + j \leq k + j \\ &\Rightarrow i + h \leq j + h \leq k + j\end{aligned}$$

Si ha

$$\begin{aligned}A &= \{i \in \mathbb{N}^n \mid i \leq j\} \subseteq \{i \in \mathbb{N}^n \mid i_1 + \dots + i_n < j_1 + \dots + j_n\} \cup \{i \in \mathbb{N}^n \mid i_1 + \dots + i_n = j_1 + \dots + j_n\} = \\ &= \{i \in \mathbb{N}^n \mid i_1 + \dots + i_n \leq j_1 + \dots + j_n\}\end{aligned}$$

Ma e' chiaro che quest'ultimo insieme e' finito.

Nota¹⁸

□

Definition 4.3. Sia $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$, $\underline{x} = (x_1, \dots, x_n)$, f non nullo.

Definiamo il *leading term* di $f(\underline{x})$:

$$LT(f) \text{ e' il termine di } f(\underline{x}) \text{ t.c. } a \leq LT(f) \quad \forall a(\underline{x}) \text{ termine di } f(\underline{x})$$

ovvero

$$LT(f) = \max_{\leq} \{a(\underline{x}) \text{ termine di } f(\underline{x})\}$$

Poiche' $\leq$ e' un ordinamento totale (vedi [4.2,pg.70]), $LT(f)$ esiste ed e' unico.

¹⁸Se la relazione $\leq$ fosse stata puramente lessicografica, senza il controllo sul grado di $\underline{x}$, allora la 3. diventava falsa, infatti, si avrebbe

$$(0, n) \leq (1, 0) \quad \forall n \in \mathbb{N}$$

Invece, il controllo sul grado garantisce che:

$$0 + n > 1 + 0 \quad \forall n < 1 \Rightarrow (1, 0) \leq (0, n) \quad \forall n > 1$$

Proposition 4.4. Sia $f, g \in F[x_1, \dots, x_n]$, si ha

$$\begin{aligned} \text{LT}(fg) &= \text{LT}(f)\text{LT}(g) \\ \text{LT}(f^m) &= \text{LT}(f)^m \quad \forall m \in \mathbb{N} \end{aligned}$$

Proof: Usando la notazione introdotta in [4.2, pg. 70], sia

$$\begin{aligned} \text{LT}(f) &= a\underline{x}^i, \quad i = (i_1, \dots, i_n) \\ \text{LT}(g) &= b\underline{x}^j, \quad j = (j_1, \dots, j_n) \end{aligned}$$

Si ha

$$\text{LT}(f)\text{LT}(g) = ab\underline{x}^{i+j}$$

Sia $k(\underline{x}) = c\underline{x}^k$, $k = (h_1, \dots, h_n)$ un qualsiasi termine di fg .

$k(\underline{x})$ termine di $fg \Rightarrow \exists f_1(\underline{x}), g_1(\underline{x})$ termini di $f(\underline{x}), g(\underline{x})$ t.c $k(\underline{x}) = f_1(\underline{x})g_1(\underline{x})$

dove $f_1(\underline{x}) = \alpha\underline{x}^r$, $g_1(\underline{x}) = \beta\underline{x}^s$

$k(\underline{x}) = f_1(\underline{x})g_1(\underline{x}) \Rightarrow k(\underline{x}) = \alpha\beta\underline{x}^{r+s}$

$$\begin{cases} \text{LT}(f) \leq f_1 \\ \text{LT}(g) \leq g_1 \end{cases} \Leftrightarrow \begin{cases} a\underline{x}^i \leq \alpha\underline{x}^r \\ b\underline{x}^j \leq \beta\underline{x}^s \end{cases} \xRightarrow{[4.2, \text{pg. 70}]} ab\underline{x}^{i+j} \leq \alpha\beta\underline{x}^{r+s} \Leftrightarrow \text{LT}(f)\text{LT}(g) \leq k$$

Per l'arbitrarietà di $k(\underline{x})$, termine di fg , e per la definizione di LT, si ha quindi

$$\text{LT}(f)\text{LT}(g) = \text{LT}(fg)$$

Infine,

$$\text{LT}(f^m) = \text{LT}(ff \dots f) = \text{LT}(f)\text{LT}(f) \dots \text{LT}(f) = \text{LT}(f)^m$$

□

Definition 4.5. Sia $f \in F[x_1, \dots, x_n]$, $\underline{x} = (x_1, \dots, x_n)$.

$$\begin{aligned} f \text{ e' simmetrico} &\stackrel{\text{def}}{\Leftrightarrow} f(\underline{x}) = f(\sigma(\underline{x})) \quad \forall \sigma \in S_n \\ \text{dove } \sigma(\underline{x}) &= (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \end{aligned}$$

S_n gruppo delle permutazioni di n elementi. In pratica un polinomio e' simmetrico, se resta uguale effettuando un qualsiasi scambio di variabili.

I polinomi simmetrici elementari sono:

$$\sigma_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n$$

$$\sigma_2(x_1, \dots, x_n) = \sum_{i < j} x_i x_j$$

$$\sigma_3(x_1, \dots, x_n) = \sum_{i_1 < i_2 < i_3} x_{i_1} x_{i_2} x_{i_3}$$

...

$$\sigma_h(x_1, \dots, x_n) = \sum_{i_1 < i_2 < \dots < i_h} x_{i_1} x_{i_2} \dots x_{i_h}$$

...

$$\sigma_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n$$

In pratica, i monomi di σ_h , sono tutti i possibili monomi formati da h indeterminate distinte,

ovvero

$$\bar{n} = \{1, 2, \dots, n\}$$

$$\underbrace{\{i_1, \dots, i_h\}}_{\text{tutti distinti}} \subseteq \bar{n} \Leftrightarrow x_{i_1} x_{i_2} \dots x_{i_h} \text{ e' un monomio di } \sigma_h$$

I monomi di σ_h sono quindi in numero

$$\binom{n}{h}$$

Proposition 4.6.

$$\text{LT}(\sigma_h) = x_1 x_2 \dots x_h$$

Proof: Poiche' ogni monomio di σ_h ha lo stesso numero di indeterminate, con esponente 1, distinte, si ha che per ogni $m(x)$ monomio di σ_h

$$\deg m(x) = h$$

Quindi per confrontare i monomi con $\leq$, basta usare l'ordinamento lessicografico stretto.

$$x_1^0 x_{i_1} x_{i_2} \dots x_{i_h} \leq x_1 x_2 \dots x_h \quad \forall 1 < i_1 < i_2 < \dots < i_h$$

$$x_1 x_2^0 x_{i_2} \dots x_{i_h} \leq x_1 x_2 \dots x_h \quad \forall 1 = i_1 < 2 < i_2 < \dots < i_h$$

$$x_1 x_2 x_3^0 x_{i_3} \dots x_{i_h} \leq x_1 x_2 x_3 \dots x_h \quad \forall 1 = i_1 < 2 = i_2 < 3 < i_3 < \dots < i_h$$

...

$$x_1 x_2 x_3 x_{i_3} \dots x_{i_{h-1}} x_h^0 x_{i_h} \leq x_1 \dots x_h \quad \forall 1 = i_1 < 2 = i_2 < 3 = i_3 < \dots < h-1 = i_{h-1} < h < i_h$$

$$x_1 x_2 \dots x_h = x_1 \dots x_h \quad \forall 1 = i_1 < 2 = i_2 < 3 = i_3 < \dots < h-1 = i_{h-1} < h = i_h$$

□

Proposition 4.7. *Formule di Viete'.*

Sia $f(x) = a_0 + a_1 x + \dots + x^d \in F[x]$ monico, $K = CS(f(x), F)$ e siano

$$\alpha_1, \dots, \alpha_d \in K$$

tutte le radici di $f(x)$, allora

$$a_h = (-1)^{d-h} \sigma_{d-h}(\alpha_1, \dots, \alpha_d) \quad \forall h = 0, \dots, d-1$$

ovvero

$$f(x) = x^d + \sum_{h=0}^{d-1} (-1)^{d-h} \sigma_{d-h}(\alpha_1, \dots, \alpha_d) x^h$$

dove σ_h e' il polinomio elementare h -esimo.

Proof:

$$f(x) = a_0 + a_1 x + \dots + x^d \quad (1)$$

$$K = CS(f(x), F) \Rightarrow f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_d) = (x^d + \dots) \quad (2)$$

Calcoliamo i termini dentro l'ultima parentesi.

1. Termine di grado $d-1$: poiche' dobbiamo arrivare a x^{d-1} , dai vari fattori di primo grado dobbiamo selezionare almeno $d-1$ indeterminate x . Ad esempio, se nella prima parentesi scegliamo $-\alpha_1$, in tutte le altre dobbiamo prendere solo x , avremo quindi $-\alpha_1 x^{d-1}$.

Quindi, ad ogni scelta stiamo scegliendo una α_i e tutte le altre saranno necessariamente delle x . Il termine sara' la somma di tutte le scelte:

$$-\alpha_1 x^{d-1} - \alpha_2 x^{d-1} - \dots - \alpha_d x^{d-1} = -\left(\sum \alpha_i\right) x^{d-1}$$

E per la def [4.5,pg.71], e' proprio

$$-\sigma_1(\alpha_1, \dots, \alpha_d) x^{d-1}$$

2. Termine di grado $d-2$: ragionando come prima notiamo che ad ogni scelta possiamo scartare arbitrariamente due distinte α_i, α_j , quindi il termine sara' la somma di tutte le distinte coppie estratte da $\alpha_1, \dots, \alpha_d$. Stavolta pero' il segno sara' positivo, perche' $(-\alpha_i)(-\alpha_j) = \alpha_i \alpha_j$. In definitiva:

$$\left(\sum_{i < j} \alpha_i \alpha_j\right) x^{d-2}$$

E per la def [4.5,pg.71], e' proprio

$$\sigma_2(\alpha_1, \dots, \alpha_d) x^{d-2}$$

3. Termine di grado $d-h$, $0 < h$: il termine sara' la somma di tutte le h -uple (non ordinate) $\alpha_{i_1}, \dots, \alpha_{i_h}$. Il segno sara' positivo se h e' pari, negativo altrimenti. Quindi:

$$(-1)^h \left(\sum_{i_1 < i_2 < \dots < i_h} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_h}\right) x^{d-h}$$

E per la def [4.5,pg.71], e' proprio

$$(-1)^h \sigma_h(\alpha_1, \dots, \alpha_d) x^{d-h}$$

Confrontando i coefficienti della (1) e quelli della (2) si ha la tesi. $\square$

Theorem 4.8. Sia $f \in F[x_1, \dots, x_n]$ un polinomio simmetrico, $\underline{x} = (x_1, \dots, x_n)$. Si ha

$$\exists! g \in F[x_1, \dots, x_n] : f(\underline{x}) = g(\sigma_1(\underline{x}), \sigma_2(\underline{x}), \dots, \sigma_n(\underline{x}))$$

Dove σ_i sono i polinomi simmetrici elementari.

Proof: Non dimostriamo l'unicita'.

Sia

$$\underline{x} = (x_1, \dots, x_n)$$

$$h = (h_1, \dots, h_n) \in \mathbb{N}^n$$

$$g(\underline{x}) = \text{LT}(f) = a \underline{x}^h = a x_1^{h_1} \dots x_n^{h_n} \quad (1)$$

(1) $h_1 \geq h_2 \geq \dots \geq h_n$

Supponiamo per assurdo $h_i < h_{i+1}$. Sia $\sigma = (i, i+1)$ la trasposizione che scambia i con $i+1$.

$$\begin{cases} f(\underline{x}) \text{ simmetrico} \\ g(\underline{x}) \text{ termine di } f(\underline{x}) \end{cases} \Rightarrow g(\sigma(\underline{x})) \text{ e' ancora un termine di } f(\underline{x})$$

$$(1) \Rightarrow g(\sigma(\underline{x})) = g(x_1, \dots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \dots, x_n) = a x_1^{h_1} \dots x_{i-1}^{h_{i-1}} x_i^{h_{i+1}} x_{i+1}^{h_i} x_n^{h_n}$$

$$\underbrace{\Rightarrow}_{h_{i+1} > h_i} g(\sigma(\underline{x})) > g(\underline{x}) = \text{LT}(f)$$

assurdo contro la definizione di LT.

Sia

$$\varphi_1 = a \sigma_1^{h_1-h_2} \sigma_2^{h_2-h_3} \sigma_3^{h_3-h_4} \dots \sigma_{n-1}^{h_{n-1}-h_n} \sigma_n^{h_n}$$

che e' una scelta lecita poiche' $h_1 \geq h_2 \geq \dots \geq h_n$.

$$\begin{aligned}
\text{LT}(\varphi_1) &\stackrel{[4.4, \text{pg.71}]}{=} a\text{LT}(\sigma_1^{h_1-h_2}) \dots \text{LT}(\sigma_{n-1}^{h_{n-1}-h_n}) \text{LT}(\sigma_n^{h_n}) = \\
&\stackrel{[4.4, \text{pg.71}]}{=} a\text{LT}(\sigma_1)^{h_1-h_2} \dots \text{LT}(\sigma_{n-1})^{h_{n-1}-h_n} \text{LT}(\sigma_n)^{h_n} = \\
&\stackrel{[4.6, \text{pg.72}]}{=} ax_1^{h_1-h_2} (x_1x_2)^{h_2-h_3} (x_1x_2x_3)^{h_3-h_4} \dots (x_1 \dots x_{n-1})^{h_{n-1}-h_n} (x_1 \dots x_n)^{h_n} = \\
&= x_1^{h_1} x_2^{h_2} \dots x_n^{h_n} = \text{LT}(f)
\end{aligned}$$

$$\text{LT}(\varphi_1) = \text{LT}(f) \Rightarrow f - \varphi_1 = 0 \vee \text{LT}(f - \varphi_1) < \text{LT}(f) \quad (2)$$

(2) φ_1 e' simmetrico

$$\begin{aligned}
\varphi_1(\underline{x}) &= a\sigma_1(\underline{x})^{h_1-h_2} \dots \sigma_n(\underline{x})^{h_n} \Rightarrow \\
\Rightarrow \varphi_1(\sigma(x)) &= a\sigma_1(\sigma(x))^{h_1-h_2} \dots \sigma_n(\sigma(x))^{h_n} \stackrel{\sigma_i \text{ e' simmetrico}}{=} a\sigma_1(\underline{x})^{h_1-h_2} \dots \sigma_n(\underline{x})^{h_n} = \varphi_1(\underline{x})
\end{aligned}$$

Quindi, effettuando uno scambio di variabili in φ_1 ,

Poniamo $f_1 = f - \varphi_1$

$$f, \varphi_1 \text{ simmetrici} \Rightarrow f_1 \text{ simmetrico}$$

Possiamo allora riapplicare l'intero ragionamento fin qui svolto a f_1 , ottenendo

$$f_2 = f_1 - \varphi_2 = f - \varphi_1 - \varphi_2$$

cosi' procedendo arriviamo a

$$f_j = f - (\varphi_1 + \varphi_2 + \dots + \varphi_j)$$

Dalla (2) si ha

$$f_j = 0 \vee \text{LT}(f_j) < \text{LT}(f_{j-1}) < \dots < \text{LT}(f_1) < \text{LT}(f) \quad (2.1)$$

Quindi se per assurdo $f_j \neq 0 \quad \forall j$, avremo un numero infinito di f_j tali che $\text{LT}(f_j) < \text{LT}(f)$, e questo e' in contrasto con la 3. della prop [4.2,pg.70].

Quindi $\exists k : f_k = 0$, ovvero

$$f_k = 0 \Leftrightarrow f = \varphi_1 + \dots + \varphi_k$$

che, per costruzione degli φ_i , e' proprio il polinomio $g(\underline{x})$ della tesi. $\square$

5 Estensioni normali

Proposition 5.1. Sia $F \preceq K$ una estensione di campi, $f(x) \in F[x]$, $\underline{x} = (x_1, \dots, x_d)$, $p(\underline{x}) \in F[x_1, \dots, x_d]$, $K = CS(f(x), F)$.

Si ha

$$\begin{aligned}
p(\underline{x}) \text{ simmetrico} &\Rightarrow p(\alpha_1, \dots, \alpha_d) \in F \\
\text{dove } \alpha_1, \dots, \alpha_d &\in K \text{ sono tutte le radici di } f(x)
\end{aligned}$$

Proof: Sia $\alpha = (\alpha_1, \dots, \alpha_d)$. Ricordiamo il seguente omomorfismo di anelli:

$$\begin{aligned}
F[x_1, \dots, x_d] &\longrightarrow F[\alpha_1, \dots, \alpha_d] \\
g(x_1, \dots, x_d) &\xrightarrow{\phi} g(\alpha_1, \dots, \alpha_d) = g(\alpha)
\end{aligned}$$

Si ha

$$p(\underline{x}) \text{ simmetrico} \underbrace{\Rightarrow}_{[4.8, \text{pg. } 73]} p(\underline{x}) = \bar{p}(\sigma_1(\underline{x}), \sigma_2(\underline{x}), \dots, \sigma_d(\underline{x})) \quad (1)$$

Sia $\varphi(x)$ la parte monica di $f(x)$, ovvero $f(x) = a\varphi(x)$, $\varphi(x)$ monico

Per la [4.7, pg. 72] :

$$\varphi(x) = x^d + \sum_{h=0}^{d-1} (-1)^{d-h} \sigma_{d-h}(\alpha) x^h \underbrace{\Rightarrow}_{\varphi(x) \in F[x]} \sigma_i(\alpha) \in F[x] \quad \forall i = 1, \dots, d \quad (2)$$

$$p(\alpha) = \phi(p) \underbrace{=}_{(1), \phi \text{ omomorfismo}} \bar{p}(\phi(\sigma_1), \dots, \phi(\sigma_d)) = p(\sigma_1(\alpha), \dots, \sigma_d(\alpha))$$

$$p(\alpha) = p(\sigma_1(\alpha), \dots, \sigma_d(\alpha)) \quad (3)$$

$$\begin{cases} p(\underline{x}) \in F[x] \\ (3), (2) \end{cases} \Rightarrow p(\alpha) \in F$$

□

Definition 5.2. Sia $F \preceq K$ una estensione algebrica

$$F \preceq K \text{ e' normale} \stackrel{\text{def}}{\Leftrightarrow} \left(f(x) \in F[x], \text{ irriducibile}, \exists \alpha_1 \in K : f(\alpha_1) = 0 \Rightarrow \forall \alpha \in CS(f(x), F) : f(\alpha) = 0 \quad \alpha \in K \right)$$

In altre parole, se $F \preceq K$ e' normale, ogni polinomio irriducibile in $F[x]$ con almeno una radice in K , avra' tutte le altre radici in K .

Lemma 5.3. Sia F campo. Si ha

$$\forall f(x) \in F[x] \quad F \preceq CS(f(x), F) \text{ e' normale}$$

Proof: Sia $K = CS(f(x), F)$. Sia $g(x) \in F[x]$ irriducibile, con $\beta \in K : g(\beta) = 0$. Dimostriamo che tutte le altre radici di g stanno in K .

Siano

$$\alpha_1, \dots, \alpha_n \in K \text{ le radici di } f(x) \quad (1)$$

Si ha

$$K = \succeq f(x)F = F(\alpha_1, \dots, \alpha_n)$$

$$(1) \Rightarrow \alpha_1, \dots, \alpha_n \text{ algebrici su } F \underbrace{\Rightarrow}_{[2.43, \text{pg. } 31]} F \preceq K = F(\alpha_1, \dots, \alpha_n) \underbrace{=}_{[2.36, \text{pg. } 27]} F[\alpha_1, \dots, \alpha_n]$$

$$\beta \in K = F[\alpha_1, \dots, \alpha_n] \Rightarrow \beta = h(\alpha_1, \dots, \alpha_n)$$

Sia

$$\alpha = (\alpha_1, \dots, \alpha_n)$$

$$\underline{x} = (x_1, \dots, x_n), \quad x_i \text{ indeterminata}$$

$$s(x) = \prod_{\sigma \in S_n} (x - h(\sigma(\alpha))) \in K[x] \quad (4)$$

dove S_n e' il gruppo delle permutazioni di n elementi. E' chiaro che $s(\beta) = 0$, poiche' $x - h(\alpha)$ e' un fattore di $s(x)$.

$$(1) \quad s(x) \in F[x]$$

Consideriamo

$$S(\underline{x}, x) = \prod_{\sigma \in S_n} (x - h(\sigma(\underline{x}))) \in F[x_1, \dots, x_n, x]$$

$S(\underline{x}, x)$ e' per costruzione simmetrico nelle variabili $x_1, \dots, x_n$ (2)

$$S(\underline{x}, x) \in F[x_1, \dots, x_n][x] \Rightarrow S(\underline{x}, x) = \sum_{i=0}^{n!} p_i(\underline{x})x^i, \quad p_i(\underline{x}) \in F[x_1, \dots, x_n] \quad \forall i = 1, \dots, n!$$

$$(2) \Rightarrow \forall \sigma \in S_n \quad S(\underline{x}, x) = S(\sigma(\underline{x}), x) \Leftrightarrow \forall \sigma \in S_n \quad \sum_{i=0}^{n!} p_i(\underline{x})x^i = \sum_{i=0}^{n!} p_i(\sigma(\underline{x}))x^i \Leftrightarrow \forall \sigma \in S_n \quad \begin{cases} p_1(\underline{x}) = p_1(\sigma(\underline{x})) \\ p_2(\underline{x}) = p_2(\sigma(\underline{x})) \\ \dots \\ p_{d!}(\underline{x}) = p_{d!}(\sigma(\underline{x})) \end{cases} \Rightarrow$$

$$\Rightarrow p_i(\underline{x}) \text{ e' simmetrico } \quad \forall i = 1, \dots, n! \quad \underbrace{\Rightarrow}_{[5.1, \text{pg.74}]} \quad p_i(\alpha) \in F \quad \forall i = 1, \dots, n! \Rightarrow S(\alpha, x) \in F[x]$$

$$s(x) = S(\alpha, x) \in F[x]$$

(2) Q.E.D.

Sia $\gamma(x)$ la parte monica di $g(x)$, ovvero

$$g(x) = b\gamma(x), \quad \gamma(x) \in F[x] \text{ monico, } b \neq 0$$

Si ha

$$g(x) \text{ irrid. in } F[x] \Rightarrow \gamma(x) \text{ irrid. in } F[x]$$

$$g(\beta) = 0 \Rightarrow \gamma(\beta) = 0$$

$$\gamma(x) \in F[x] \text{ monico}$$

$$\underbrace{\Rightarrow}_{[2.30, \text{pg.24}]} \quad \gamma(x) = P_{\min}(\beta, F) \quad (3)$$

$$s(\beta) = 0, \quad s(x) \in F[x], \quad (3) \quad \underbrace{\Rightarrow}_{[2.28, \text{pg.23}]} \quad \gamma(x) / s(x) \Rightarrow$$

$$\underbrace{\Rightarrow}_{(4)} \quad \gamma(x) = (x - \tau_1(\alpha))(x - \tau_2(\alpha)) \dots (x - \tau_m(\alpha)) \in K[x] \text{ per qualche } \tau_1, \dots, \tau_m \in S_n \Rightarrow$$

$$\underbrace{\Rightarrow}_{(4)} \quad \tau_i(\alpha) \in K \quad \forall i = 1, \dots, m$$

Quindi $\gamma(x)$ ha tutte le radici in K .

□

Example 5.4. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ non e' normale, infatti,

$$x^3 - 2 \text{ e' irrid. in } \mathbb{Q}, \text{ ha } \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) \text{ come radice}$$

ma tutte le sue altre radici sono

$$\omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$$

Theorem 5.5. Sia $F \preceq K$ una estensione, allora

$$F \preceq K \text{ normale, finita} \Leftrightarrow \exists f(x) \in F[x] : K = CS(f(x), F)$$

In particolare, dati $\alpha_1, \dots, \alpha_n \in K$ algebrici su F , con $K = F(\alpha_1, \dots, \alpha_n)$, si ha

$$F \preceq K \text{ normale, finita} \Rightarrow K = CS \left(\prod_{i=1}^n P_{\min}(\alpha_i, F), F \right)$$

Proof:

(1) Dim. $\Leftarrow$

Per il lem [5.3,pg.75], $F \preceq K$ e' normale. Inoltre,

$$K = CS(f(x), F) = F(\alpha_1, \dots, \alpha_n)$$

$$\alpha_1, \dots, \alpha_n \text{ radici di } f(x) \Rightarrow \alpha_1, \dots, \alpha_n \text{ algebrici su } F[x] \xRightarrow{[2.42, \text{pg.30}]} F \preceq F(\alpha_1, \dots, \alpha_n) = K \text{ finita}$$

(1) Dim. $\Rightarrow$

$$F \preceq K \text{ finita} \Rightarrow \exists \alpha_1, \dots, \alpha_n \in K : K = F(\alpha_1, \dots, \alpha_n) \text{ algebrica} \Rightarrow \exists p_i(x) = P_{\min}(\alpha_i, F) \quad \forall i = 1, \dots, n$$

Siano date le radici dei p_i :

$$\alpha_{11} = \alpha_1, \alpha_{12}, \dots, \alpha_{1r_1}$$

$$\alpha_{21} = \alpha_2, \alpha_{22}, \dots, \alpha_{2r_2}$$

...

$$\alpha_i \in K \xRightarrow{F \preceq K \text{ normale}} \alpha_{ij} \in K \quad \forall j = 1, \dots, r_j$$

$$\Rightarrow K \supseteq CS(p_1(x)p_2(x) \dots p_n(x), F)$$

$$CS(p_1(x)p_2(x) \dots p_n(x), F) = F(\alpha_{ij}, \forall i, j) \supseteq K = F(\alpha_1, \dots, \alpha_n)$$

$$\Rightarrow K = CS(p_1(x)p_2(x) \dots p_n(x), F)$$

Quindi il polinomio cercato e'

$$f(x) = p_1(x)p_2(x) \dots p_n(x)$$

□

Proposition 5.6. Sia $F \preceq K$ una estensione,

$$[K : F] = 2 \Rightarrow F \preceq K \text{ e' normale}$$

Proof: Sia $f(x) \in F[x]$ irriducibile, con $\alpha_1 \in K$, $f(\alpha_1) = 0$.

$$f(x) = a \underbrace{\bar{f}(x)}_{\text{monico}}$$

$$\bar{f}(\alpha_1) = 0, \bar{f} \in F[x] \text{ irrid.} \xRightarrow{[2.30, \text{pg.24}]} \bar{f}(x) = P_{\min}(\alpha_1, F) \Rightarrow [F(\alpha_1) : F] = \deg \bar{f} \quad (1)$$

$$\begin{cases} \alpha_1 \in K \\ F \preceq K \end{cases} \Rightarrow F(\alpha_1) \subseteq K \Rightarrow F(\subseteq F(\alpha_1) \subseteq K \Rightarrow [F(\alpha_1) : F] \leq [K : F] = 2 \xRightarrow{(1)} \deg \bar{f} \leq 2$$

$$\bar{f} \text{ irrid.} \Rightarrow \deg \bar{f} \geq 1$$

Se $\deg \bar{f} = 1$, allora

$$f(x) = x - \alpha_1$$

e quindi $\bar{f}$ ha tutte le radici in K .

Se $\deg \bar{f} = 2$, allora

$$\bar{f}(\alpha_1) = 0 \xRightarrow{\text{Ruffini}} x - \alpha_1 \mid \bar{f} \text{ in } K[x] \xLeftrightarrow{\deg \bar{f}=2} \bar{f}(x) = (x - \alpha_1)(x - \alpha_2), \quad x - \alpha_2 \in K[x] \Rightarrow \alpha_1, \alpha_2 \in K[x]$$

e quindi f ha tutte le radici in K .
In definitiva, per l'arbitrarietà di $f(x)$, $F \preceq K$ e' normale. $\square$

6 Gruppo di Galois

Definition 6.1. Sia $F \preceq K$ una estensione algebrica. Definiamo i seguenti insiemi:

$$\begin{aligned}\mathcal{I}(K, F) &= \{\varphi : K \longrightarrow \overline{F} \mid \varphi|_F = \text{id}, \varphi \text{ omomorfismo}\} \\ \mathcal{G}(K, F) &= \{\varphi : K \longrightarrow K \mid \varphi|_F = \text{id}, \varphi \text{ isomorfismo}\}\end{aligned}$$

$\mathcal{G}(K, F)$ e' chiamato *Gruppo di Galois*.

Example 6.2.

$$\begin{aligned}\mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) &= \{\text{id}, f\} \\ \text{con } f(a + ib) &= a - ib\end{aligned}$$

Proof: Stiamo ricercando tutti gli omomorfismi del tipo

$$\begin{aligned}\varphi : \mathbb{Q}(i) &\longrightarrow \overline{\mathbb{Q}} \\ \varphi|_{\mathbb{Q}} &= \text{id}\end{aligned}$$

Poiche' $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$,

$$\varphi(a + ib) = \varphi(a) + \varphi(i)\varphi(b) \underset{\varphi|_{\mathbb{Q}}=\text{id}}{=} a + b\varphi(i)$$

$$\begin{cases} \varphi(i^2) = \varphi(i)^2 \\ \varphi(i^2) \underset{i^2=-1}{=} \varphi(-1) = -1 \end{cases} \Rightarrow \varphi(i)^2 = -1 \Leftrightarrow \varphi(i) = \pm i$$

Abbiamo quindi due possibilita. Se scegliamo $\varphi(i) = i$, allora $\varphi = \text{id}$, altrimenti $\varphi = f$.

Resta da verificare che f e' un omomorfismo. Intanto f e' una funzione ben definita, perche' ogni elem, di $\mathbb{Q}(i)$ si scrive in modo unico come $a + ib$ (vedi [2.35,pg.26])

$$\begin{aligned}f(a + ib + c + id) &= f((a + c) + i(b + d)) = (a + c) - i(b + d) = a - ib + c - id = f(a + ib) + f(c + id) \\ f((a + ib)(c + id)) &= f(ac - bd + i(ad + bc)) = ac - bd - i(ad + bc) = (a - ib)(c - id) = f(a + ib)f(c + id)\end{aligned}$$

$\square$

Proposition 6.3. Sia $F \preceq K$ algebrica. Si ha

$$\begin{aligned}\varphi \in \mathcal{I}(K, F) &\Rightarrow \varphi : K_F \longrightarrow \overline{F}_F \text{ e' una applicazione lineare iniettiva} \\ \varphi \in \mathcal{G}(K, F) &\Rightarrow \varphi : K_F \longrightarrow K_F \text{ e' un isomorfismo vettoriale}\end{aligned}$$

Proof:

$$F \text{ campo} \underset{[1.1, \text{pg.1}]}{\Rightarrow} F \neq \{0\}$$

$$\varphi \in \mathcal{I}(K, F) \Rightarrow \varphi|_F = \text{id} \underset{F \neq \{0\}}{\Rightarrow} \text{Im } \varphi \neq \{0\} \underset{[AI, 18.2, \text{pg.90}]}{\Rightarrow} \varphi \text{ e' iniettiva}$$

$$\varphi \in \mathcal{I}(K, F) \Rightarrow \begin{cases} \varphi : K \longrightarrow \overline{F} \\ \varphi|_F = \text{id} \\ F \preceq K, \overline{F} \end{cases} \underset{[2.15, \text{pg.15}]}{\Rightarrow} \varphi \text{ e' una applicazione lineare}$$

Analogamente nel caso in cui $\varphi \in \mathcal{G}(K, F)$. L'unica differenza e' che per definizione φ e' biettiva. $\square$

Proposition 6.4. Sia $F \preceq K$ algebrica,

1. $\mathcal{G}(K, F) \subseteq \mathcal{I}(K, F)$
2. $(\mathcal{G}(K, F), \circ)$ e' un gruppo
3. $F \preceq L \preceq K \Rightarrow \mathcal{G}(K, L) \underbrace{\leq}_{\text{sottogruppo}} \mathcal{G}(K, F)$

dove $\circ$ e' l'operazione di composizione.

Proof:

(1) Dim 1.

Basta dimostrare che $K \subseteq \overline{F}$

$$F \preceq K \text{ algebrica} \underbrace{\Rightarrow}_{[2.62, \text{pg.49}]} \overline{F} = \overline{K} \supseteq K$$

(2) Dim 2.

Siano $f, g \in \mathcal{G}(K, F)$

fg e' ancora un omomorfismo

$$\begin{aligned} \{\alpha \in F \Rightarrow fg(\alpha) = f(\alpha) = \alpha\} &\Rightarrow fg|_F = \text{id} \\ &\Rightarrow fg \in \mathcal{G}(K, F) \end{aligned}$$

$\circ$ e' associativa

id e' l'elemento neutro

$$f|_F = \text{id} \Rightarrow \text{Im } f \neq \{0\}$$

$$f \text{ isomorfismo} \Rightarrow \exists f^{-1}$$

(3) Dim 3.

Intanto osserviamo che

$$F \preceq K \text{ algebrica} \underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} L \preceq K \text{ algebrica}$$

Poiche' $\mathcal{G}(K, L), \mathcal{G}(K, F)$ sono entrambi due gruppi con la stessa operazione, basta controllare che $\mathcal{G}(K, L) \subseteq \mathcal{G}(K, F)$.

$$g \in \mathcal{G}(K, L) \Rightarrow \begin{cases} g : K \longrightarrow K \text{ isomorf.} \\ g|_L = \text{id} \underbrace{\Rightarrow}_{F \subseteq L} g|_F = \text{id} \end{cases} \Rightarrow g \in \mathcal{G}(K, F)$$

□

Proposition 6.5.

$$\begin{cases} F \preceq K \text{ algebrica} \\ F \preceq L \preceq K \end{cases} \Rightarrow \mathcal{I}(K, L) \subseteq \mathcal{I}(K, F)$$

Proof:

$$\varphi \in \mathcal{I}(K, L) \Rightarrow \varphi|_L = \text{id} \underbrace{\Rightarrow}_{F \subseteq L} \varphi|_F = \text{id}$$

$$F \preceq K \text{ algebrica} \underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} F \preceq L \text{ algebrica} \underbrace{\Rightarrow}_{[2.62, \text{pg.49}]} \overline{F} = \overline{L}$$

$$\varphi \in \mathcal{I}(K, L) \Rightarrow \varphi : K \longrightarrow \overline{L} = \overline{F}$$

$$\begin{cases} \varphi : K \longrightarrow \overline{F}, \text{ omomorfismo} \\ \varphi|_F = \text{id} \end{cases} \Rightarrow \varphi \in \mathcal{I}(K, F)$$

□

Proposition 6.6. *Sia*

1. $F \preceq K$ *algebraica*, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$

2. $\varphi : F \longrightarrow \overline{F}$ *una immersione e*

$$\begin{aligned} \Phi : F[x] &\longrightarrow \overline{F}[x] \\ \sum_{i=0}^r a_i x^i &\mapsto \sum_{i=0}^r \varphi(a_i) x^i \end{aligned}$$

l'omomorfismo indotto da φ (vedi [1.13, pg. 3])

3. $f(x) \in F[x]$, $a \in K$

4. $\tilde{\varphi} : K \longrightarrow \overline{F}$ *un omomorfismo t.c. $\tilde{\varphi}|_F = \varphi$*

allora si ha

$$1. \tilde{\varphi}(f(a)) = \Phi(f)(\tilde{\varphi}(a))$$

$$2. \tilde{\varphi}(\alpha) \text{ e' radice di } \Phi(p)$$

In particolare, la tesi vale per qualsiasi $\tilde{\varphi} \in \mathcal{I}(K, F)$ (basta considerare $\varphi = \text{id}$), e si ha

$$\tilde{\varphi}(f(a)) = f(\tilde{\varphi}(a))$$

$$\tilde{\varphi}(\alpha) \text{ e' radice di } p(x)$$

Proof:

(1) Dim. 1.

$$f(x) \in F[x] \Rightarrow f(x) = \sum_{i=1}^r b_i x^i, \quad b_i \in F \quad \forall i = 1, \dots, r \Rightarrow \Phi(f) \underbrace{=}_{(1)} \sum_{i=1}^r \varphi(b_i) x^i \quad (1.1)$$

$$\begin{aligned} f(a) &= b_0 + b_1 a + \dots + b_r a^r \\ \tilde{\varphi}(f(a)) &\underbrace{=}_{\tilde{\varphi} \text{ omomorf.}} \tilde{\varphi}(b_0) + \tilde{\varphi}(b_1) \tilde{\varphi}(a) + \dots + \tilde{\varphi}(b_r) \tilde{\varphi}(a)^r = \\ &\underbrace{=}_{\tilde{\varphi}|_F = \varphi} \varphi(b_0) + \varphi(b_1) \tilde{\varphi}(a) + \dots + \varphi(b_r) \tilde{\varphi}(a)^r \underbrace{=}_{(1.1)} \Phi(f)(\tilde{\varphi}(a)) \end{aligned}$$

(2) Dim 2.

$$p(x) = P_{\min}(\alpha, F) \Rightarrow p(\alpha) = 0, \quad \alpha \in K \Rightarrow \tilde{\varphi}(p(\alpha)) = \tilde{\varphi}(0) = 0 \underbrace{\Leftrightarrow}_{\text{passo 1}} \Phi(p)(\tilde{\varphi}(\alpha)) = 0 \Rightarrow$$

$$\Rightarrow \tilde{\varphi}(\alpha) \in \overline{F} \text{ e' radice di } \Phi(p)$$

□

Proposition 6.7. *Sia $F \preceq K$ algebraica, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$, $\tilde{\varphi} \in \mathcal{I}(K, F)$, allora si ha*

$$\tilde{\varphi}(\alpha) \text{ e' radice di } p(x)$$

Preso $f(x) \in F[x]$, $a \in K$, si ha

$$\tilde{\varphi}(f(a)) = f(\tilde{\varphi}(a))$$

Proof: Basta rileggere la [6.6,pg.80]. □

Theorem 6.8. *Sia*

1. $F \preceq K$, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$, $n = \deg p(x)$
2. $\varphi : F \longrightarrow \overline{F}$ una immersione
3. $E = \{ \tilde{\varphi} : K \longrightarrow \overline{F} \mid \tilde{\varphi}|_F = \varphi, \tilde{\varphi} \text{ omomorfismo} \}$
4. $\Phi : F[x] \longrightarrow \overline{F}[x]$ l'omomorfismo indotto da φ e $\beta_1, \dots, \beta_n$ le radici di $\Phi(p)$

Si ha

$$\begin{cases} K = F(\alpha) \\ \alpha \text{ algebrico su } F \end{cases} \Rightarrow \begin{cases} |E| \leq n \\ |E| = | \{ \tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E \} | \text{ con biezione } \tilde{\varphi} \in E \mapsto \tilde{\varphi}(\alpha) \\ \{ \beta_1, \dots, \beta_n \} = \{ \tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E \} \end{cases}$$

$$\begin{cases} K = F(\alpha) \\ \alpha \text{ separabile e algebrico su } F \end{cases} \Rightarrow |E| = n$$

Proof: Sia

$$\begin{aligned} \Phi : F[x] &\longrightarrow \overline{F}[x] \\ \sum_{i=0}^r a_i x^i &\mapsto \sum_{i=0}^r \varphi(a_i) x^i \quad (1) \end{aligned}$$

l'omomorfismo indotto da φ (vedi [1.13,pg.3]).

Sia $\tilde{\varphi} \in E$.

(1) Sia $E' = \{ \tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E \}$. Dim che

$$|E| = |E'|$$

In altre parole, ogni $\tilde{\varphi} \in E$ e' completamente determinato da $\tilde{\varphi}(\alpha)$.

Utilizziamo la seguente funzione:

$$\begin{aligned} e : E &\longrightarrow E' \\ \tilde{\varphi} &\mapsto \tilde{\varphi}(\alpha) \end{aligned}$$

e e' chiaramente surriettiva. E' anche iniettiva: supponendo che $\tilde{\varphi}(\alpha) = \tilde{\varphi}'(\alpha)$ dimostriamo che $\tilde{\varphi} = \tilde{\varphi}'$

$$\alpha \text{ algebrico su } F \quad \underbrace{\Rightarrow}_{[2.36, \text{pg. } 27]} K = F(\alpha) = F[\alpha] \quad \underbrace{=}_{[2.40, \text{pg. } 29]} \{ b_0 + b_1 \alpha + b_2 \alpha^2 + \dots + b_{n-1} \alpha^{n-1} \mid b_i \in F \}$$

$$\beta \in K \Rightarrow b = b_0 + b_1 \alpha + b_2 \alpha^2 + \dots + b_{n-1} \alpha^{n-1}$$

$$\tilde{\varphi}(\beta) = \tilde{\varphi}(b_0) + \tilde{\varphi}(b_1) \tilde{\varphi}(\alpha) + \dots + \tilde{\varphi}(b_{n-1}) \tilde{\varphi}(\alpha)^{n-1} \quad \underbrace{=}_{\tilde{\varphi}|_F = \varphi} \varphi(b_0) + \varphi(b_1) \tilde{\varphi}(\alpha) + \dots + \varphi(b_{n-1}) \tilde{\varphi}(\alpha)^{n-1}$$

$$\tilde{\varphi}'(\beta) = \varphi(b_0) + \varphi(b_1) \tilde{\varphi}'(\alpha) + \dots + \varphi(b_{n-1}) \tilde{\varphi}'(\alpha)^{n-1} \quad \underbrace{=}_{\tilde{\varphi} = \tilde{\varphi}'} \varphi(b_0) + \varphi(b_1) \tilde{\varphi}(\alpha) + \dots + \varphi(b_{n-1}) \tilde{\varphi}(\alpha)^{n-1} = \tilde{\varphi}(\beta)$$

Per l'arbitrarieta' di b abbiamo quindi

$$\forall \beta \in K \quad \tilde{\varphi}(\beta) = \tilde{\varphi}'(\beta) \Leftrightarrow \tilde{\varphi} = \tilde{\varphi}'$$

Abbiamo

$$\begin{aligned}
n = \deg p = \deg \Phi(p) &\Rightarrow \exists \beta_1, \dots, \beta_n \text{ radici di } \Phi(p) \\
\Phi(p) \in \overline{F}[x], \overline{F} \text{ chiuso} &\Rightarrow \beta_i \in \overline{F} \quad \forall i = 1, \dots, n \quad (2) \\
&\quad [2.56, \text{pg.42}] \\
p(x) = P_{\min}(\alpha, F) &\Rightarrow \tilde{\varphi}(\alpha) \in \overline{F} \text{ e' radice di } \Phi(p) \Rightarrow \exists i : \beta_i = \tilde{\varphi}(\alpha) \\
&\quad [6.6, \text{pg.80}] \quad (2)
\end{aligned}$$

Quindi, fin qui abbiamo visto che

$$\begin{aligned}
\tilde{\varphi} \in E &\Rightarrow \tilde{\varphi}(\alpha) \in \{\beta_1, \dots, \beta_n\} \\
&\Rightarrow \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\} \subseteq \{\beta_1, \dots, \beta_n\} \Rightarrow |\{\beta_1, \dots, \beta_n\}| \geq |\{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}| \underbrace{=}_{\text{passo 1}} |E| \quad (3)
\end{aligned}$$

$$\beta_1, \dots, \beta_n \text{ possono non essere distinti} \Rightarrow |\{\beta_1, \dots, \beta_n\}| \leq n \underbrace{\Rightarrow}_{(3)} |E| \leq n$$

che e' la prima parte della tesi.

(2) Dim. che

$$\{\beta_1, \dots, \beta_n\} = \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}$$

Per completare l'uguaglianza in (3), dimostriamo che $\{\beta_1, \dots, \beta_n\} \subseteq \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}$. Fissato $1 \leq k \leq n$, $\bar{\beta} = \beta_k$, consideriamo la funzione f definita come

$$f : K = F(\alpha) \longrightarrow \overline{F}$$

$$b_0 + b_1\alpha + b_2\alpha^2 + \dots + b_{n-1}\alpha^{n-1} \mapsto \varphi(b_0) + \varphi(b_1)\bar{\beta} + \varphi(b_2)\bar{\beta}^2 + \dots + \varphi(b_{n-1})\bar{\beta}^{n-1}$$

o in altri termini:

$$h(x) \in F[x]$$

$$f(h(\alpha)) = \Phi(h)(\bar{\beta}) \quad (4)$$

Per il lemma [2.58, pg.43], applicato a $L = F$, abbiamo che:

$$f \text{ e' un omomorfismo t.c. } f|_F = \varphi$$

quindi

$$\begin{cases} f : K \longrightarrow \overline{F} \\ f|_F = \varphi \\ f \text{ omomorfismo} \end{cases} \Rightarrow f \in E$$

Abbiamo cosi' trovato un elemento $f \in E$ tale che

$$f(\alpha) = \bar{\beta}$$

quindi $\bar{\beta} \in \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}$.

Per l'arbitrarieta' di $\bar{\beta}$ abbiamo quindi

$$\{\beta_1, \dots, \beta_n\} \subseteq \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}$$

e per la (3)

$$\{\beta_1, \dots, \beta_n\} = \{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}$$

(3) Supponiamo adesso che α sia separabile su F e dimostriamo che $|E| = n$.

$$\begin{aligned}
\varphi \text{ immersione} &\Rightarrow \varphi \text{ iniettiva} \xRightarrow{[1.13, \text{pg.3}]} \Phi \text{ iniettiva} \Rightarrow \Phi : F[x] \longrightarrow \text{Im } \Phi \text{ e' un isomorfismo } (*) \\
\alpha \text{ separabile} &\xRightarrow{\text{per def.}} p(x) \text{ separabile} \xRightarrow{(*)} \Phi(p)(x) \text{ separabile} \Rightarrow \beta_1, \dots, \beta_n \text{ sono tutte distinte} \Rightarrow \\
&\Rightarrow |\{\beta_1, \dots, \beta_n\}| = n \\
n = |\{\beta_1, \dots, \beta_n\}| &\xRightarrow{\text{passo 2}} |\{\tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E\}| \xRightarrow{\text{passo 1}} |E| \\
|E| &= n
\end{aligned}$$

□

Corollary 6.9. Sia $F \preceq K$, $\varphi : F \longrightarrow \overline{F}$ una immersione. Si ha

$$F \preceq K \text{ finita} \Rightarrow \left| \left\{ \tilde{\varphi} : K \longrightarrow \overline{F} \mid \tilde{\varphi}|_F = \varphi, \tilde{\varphi} \text{ omomorfismo} \right\} \right| \leq [K : F]$$

Inoltre, se $F \preceq K$ e' anche separabile, allora vale l'uguaglianza.

Nota: la dimostrazione e' costruttiva: viene fornito il metodo per costruire l'insieme.

Proof: Sia E l'insieme della tesi. Osserviamo intanto che

$$F \preceq K \text{ finita} \xRightarrow{[2.44, \text{pg.31}]} F \preceq K \text{ finit. gen. e algebrica}$$

(1) Supponiamo $F \preceq K$ separabile e dimostriamo che $|E| = [K : F]$

$$F \preceq K \text{ finit. gen. e separabile} \xRightarrow{[3.29, \text{pg.65}]} F \preceq K \text{ semplice} \Rightarrow K = F(\alpha), \alpha \in K$$

$$F \preceq K \text{ finita} \Rightarrow F \preceq K \text{ algebrica} \Rightarrow \alpha \text{ algebrico su } F$$

Quindi per il thm [6.8, pg.81] si ha

$$|E| = \deg P_{\min}(\alpha, F) \xRightarrow{[2.40, \text{pg.29}]} [F(\alpha) : F] = [K : F]$$

(2) Supponiamo $F \preceq K$ non separabile e dimostriamo che $|E| \leq [K : F]$

$$F \preceq K \text{ finit. gen.} \Rightarrow K = F(\alpha_1, \dots, \alpha_n)$$

$$F \preceq K \text{ algebrica} \Rightarrow \alpha_1, \dots, \alpha_n \text{ algebrici su } F$$

Procediamo per induzione su n

(2.1) $n = 1$

Basta applicare il thm [6.8, pg.81]:

$$|E| = \deg P_{\min}(\alpha_1, F) \xRightarrow{[2.40, \text{pg.29}]} [F(\alpha_1) : F] = [K : F]$$

(2.2) $n - 1 \Rightarrow n$

Sia $F' = F(\alpha_1, \dots, \alpha_{n-1})$, e sia $E' = \{ \tilde{\varphi} : F' \longrightarrow \overline{F} \mid \tilde{\varphi}|_{F'} = \varphi, \tilde{\varphi} \text{ omomorfismo} \}$, si ha $F \preceq F' \preceq F'(\alpha_n)$

Abbiamo $|E'| \leq [F' : F]$, infatti, se $F \preceq F'$ e' separabile, per il passo 1 abbiamo $|E'| = [F' : F]$, altrimenti possiamo applicare l'ipotesi induttiva, e abbiamo $|E'| \leq [F' : F]$.

$$E' = \{ \varphi'_1, \dots, \varphi'_h \}, \quad h \leq [F' : F] \quad (1)$$

Sia $\varphi'_i \in E'$, $E''_i = \{ \tilde{\varphi}' : F'(\alpha_n) \longrightarrow \overline{F'} \mid \tilde{\varphi}'|_{F'} = \varphi'_i, \tilde{\varphi}' \text{ omorf.} \}$.

(2.2.1) Sia $E'' = \bigcup_{i=1}^h E''_i$, si ha $E'' = E$

Dim. $E'' \subseteq E$.

$$\alpha_1, \dots, \alpha_{n-1} \text{ algebrici} \xRightarrow{[2.43, \text{pg.31}]} F \preceq F' = F(\alpha_1, \dots, \alpha_{n-1}) \text{ algebrica} \xRightarrow{[2.62, \text{pg.49}]} \overline{F}' = \overline{F} \quad (2)$$

$$\tilde{\varphi}' \in E''_i \Rightarrow \tilde{\varphi}'|_{F'} = \varphi'_i \xRightarrow{F \subseteq F'} \tilde{\varphi}'|_F = \varphi'_i|_F \xRightarrow{\varphi'_i \in E'} \varphi \quad (3)$$

$$F'(\alpha_n) = K$$

$$\begin{aligned} \Rightarrow E''_i &= \left\{ \tilde{\varphi}' : F'(\alpha_n) \longrightarrow \overline{F}' \mid \tilde{\varphi}'|_{F'} = \varphi'_i, \tilde{\varphi}' \text{ omorf.} \right\} = \\ &= \left\{ \tilde{\varphi}' : K \longrightarrow \overline{F} \mid \tilde{\varphi}'|_{F'} = \varphi'_i, \tilde{\varphi}'|_F = \varphi, \tilde{\varphi}' \text{ omorf.} \right\} \subseteq E \end{aligned}$$

$$\forall 0 \leq i \leq h \quad E''_i \subseteq E \Rightarrow \bigcup_{i=1}^h E''_i \subseteq E$$

Dim. $E \subseteq E''$. Sia $\tilde{\varphi} \in E$ e sia $f = \tilde{\varphi}|_{F'}$

$$f|_F = \tilde{\varphi}|_F = \varphi \Rightarrow f \in E' \Rightarrow f = \varphi'_j$$

$$\begin{cases} \tilde{\varphi} : K = F'(\alpha_n) \longrightarrow \overline{F} = \overline{F}', \text{ omorfismo} \\ \tilde{\varphi}|_{F'} = f = \varphi'_j \end{cases} \Rightarrow \tilde{\varphi} \in E''_j \subseteq E''$$

$$(2.2.2) \quad |E| \leq \sum_{i=1}^h |E''_i|$$

$$E \xRightarrow{\text{passo 2.2.1}} E'' = \bigcup_{i=1}^h E''_i \Rightarrow |E| \leq \sum_{i=1}^h |E''_i|$$

Applicando il thm [6.8,pg.81] su φ'_i e $F \subseteq F'(\alpha_n)$, abbiamo

$$|E''_i| \leq \deg P_{\min}(\alpha_n, F') = [F'(\alpha_n) : F'] \quad (*)$$

Quindi

$$|E| \xRightarrow{\text{passo 2.2.2}} \sum_{i=1}^h |E''_i| \xRightarrow{(*)} h[F'(\alpha_n) : F'] \xRightarrow{(1)} [F' : F][F'(\alpha_n) : F'] \xRightarrow{[2.18, \text{pg.16}]} [F'(\alpha_n) : F] = [K : F]$$

$$|E| \leq [K : F]$$

□

Corollary 6.10.

$$F \preceq K \text{ finita} \Rightarrow |\mathcal{G}(K, F)| \leq |\mathcal{I}(K, F)| \leq [K : F]$$

$$F \preceq K \text{ finita e separabile} \Rightarrow |\mathcal{G}(K, F)| \leq |\mathcal{I}(K, F)| = [K : F]$$

Proof: Basta applicare [6.9,pg.83], con $\varphi = \text{id}$, e la prop [6.4,pg.79].

□

Definition 6.11. Sia $F \preceq K$ algebrica e $T \subseteq \mathcal{I}(K, F)$, definiamo

$$K^T = \{\alpha \in K \mid t(\alpha) = \alpha \quad \forall t \in T\}$$

Proposition 6.12. Sia $F \preceq K$ algebrica, $L \subseteq K$ e $T \subseteq \mathcal{I}(K, F)$, si ha

1. $F \preceq K^T \preceq K$
2. $T \subseteq \mathcal{I}(K, K^T)$
3. $L \subseteq K^{\mathcal{I}(K, L)}$
4. $\mathcal{G}(K, K^{\mathcal{G}(K, F)}) = \mathcal{G}(K, F)$

Proof:

⟨1⟩ Dim 1.

$t \in T \subseteq \mathcal{I}(K, F) \Rightarrow t|_F = \text{id} \Rightarrow t(\alpha) = \alpha \quad \forall \alpha \in F \Rightarrow F \subseteq K^T \quad K^T \subseteq K$
 Resta da dimostrare che $K^T \preceq K$, ovvero che K^T e' un sottocampo di K .

$$\begin{aligned} \alpha, \beta &\in K^T \\ t(\alpha - \beta) &\underbrace{=}_{t \text{ omo.}} t(\alpha) - t(\beta) = \alpha - \beta \\ &\Rightarrow \alpha - \beta \in K^T \\ t(\alpha\beta^{-1}) &\underbrace{=}_{t \text{ omo.}} t(\alpha)t(\beta^{-1}) = t(\alpha)(t(\beta))^{-1} = \alpha\beta^{-1} \\ &\Rightarrow \alpha\beta^{-1} \in K^T \end{aligned}$$

e quindi per la [1.6,pg.1] si ha la tesi.

⟨2⟩ Dim 2.

$$\begin{aligned} t &\in T \\ t|_{K^T} &\underbrace{=}_{\text{per definizione di } K^T} \text{id} \\ \left\{ \begin{array}{l} \text{passo 1} \Rightarrow F \preceq K^T \preceq K \\ F \preceq K \text{ algebrica} \end{array} \right. &\underbrace{\Rightarrow}_{[2.45, \text{pg.31}]} F \preceq K^T \text{ algebrica} \underbrace{\Rightarrow}_{[2.62, \text{pg.49}]} \overline{F} = \overline{K^T} \\ \left\{ \begin{array}{l} t : K \longrightarrow \overline{F} = \overline{K^T} \text{ omomorfismo} \\ t|_{K^T} = \text{id} \end{array} \right. &\Rightarrow t \in \mathcal{I}(K, K^T) \end{aligned}$$

⟨3⟩ Dim 3.

$$\alpha \in L \subseteq K$$

$$(\varphi \in \mathcal{I}(K, L) \Rightarrow \varphi|_L = \text{id} \Rightarrow \varphi(\alpha) = \alpha) \Rightarrow \alpha \in K^{\mathcal{I}(K, L)}$$

⟨4⟩ Dim. 4.

⟨4.1⟩ Dim $\supseteq$

$$\begin{aligned} \varphi \in \mathcal{G}(K, F) &\Rightarrow \left\{ \begin{array}{l} \varphi : K \longrightarrow K \text{ isomorf.} \\ \varphi|_F = \text{id} \end{array} \right. \\ \alpha \in K^{\mathcal{G}(K, F)} &\Rightarrow f(\alpha) = \alpha \quad \forall f \in \mathcal{G}(K, F) \Rightarrow \varphi(\alpha) = \alpha \\ &\Rightarrow \varphi|_{K^{\mathcal{G}(K, F)}} = \text{id} \\ \left\{ \begin{array}{l} \varphi : K \longrightarrow K \text{ isomorf.} \\ \varphi|_{K^{\mathcal{G}(K, F)}} = \text{id} \end{array} \right. &\Rightarrow \varphi \in \mathcal{G}(K, K^{\mathcal{G}(K, F)}) \end{aligned}$$

⟨4.2⟩ Dim $\subseteq$

$$\begin{aligned}
\varphi \in \mathcal{G}(K, K^{\mathcal{G}(K,F)}) &\Rightarrow \begin{cases} \varphi : K \longrightarrow K \text{ isomorf.} \\ \varphi|_{K^{\mathcal{G}(K,F)}} = \text{id} \end{cases} \quad (*) \\
\mathcal{G}(K, F) \underbrace{\subseteq}_{[6.4, \text{pg.79}]} \mathcal{I}(K, F) &\underbrace{\Rightarrow}_{1.} F \preceq K^{\mathcal{G}(K,F)} \quad (**) \\
(*), (**) &\Rightarrow \varphi|_F = \text{id} \\
\begin{cases} \varphi : K \longrightarrow K \text{ isomorf.} \\ \varphi|_F = \text{id} \end{cases} &\Rightarrow \varphi \in \mathcal{G}(K, F)
\end{aligned}$$

□

Proposition 6.13. *Sia $F \preceq L \preceq K$, si ha*

$$F \preceq K \text{ separabile, finita} \Rightarrow L = K^{\mathcal{I}(K,L)}$$

Proof: Sia $m = [K : L]$

$$F \preceq K \text{ separabile, finita} \underbrace{\Rightarrow}_{[3.32, \text{pg.68}], [2.18, \text{pg.16}]} L \preceq K \text{ separabile, finita} \underbrace{\Rightarrow}_{[6.10, \text{pg.84}]} |\mathcal{I}(K, L)| = [K : L] = m \quad (1)$$

$$L \preceq K \underbrace{\Rightarrow}_{[6.12, \text{pg.84}]} L \preceq K^{\mathcal{I}(K,L)} \preceq K \quad (2)$$

$$\begin{aligned}
L \preceq K \text{ separabile, finita} &\underbrace{\Rightarrow}_{[3.32, \text{pg.68}], [3.32, \text{pg.68}]} K^{\mathcal{I}(K,L)} \preceq K \text{ separabile, finita} \Rightarrow \\
&\underbrace{\Rightarrow}_{[6.10, \text{pg.84}]} \underbrace{|\mathcal{I}(K, K^{\mathcal{I}(K,L)})|}_I = [K : K^{\mathcal{I}(K,L)}] \underbrace{\leq}_{(2), [2.18, \text{pg.16}]} [K : L] = m \quad (2.1)
\end{aligned}$$

$$|I| \leq m \quad (3)$$

$$L \preceq K \text{ finita} \underbrace{\Rightarrow}_{[2.44, \text{pg.31}]} L \preceq K \text{ algebrica} \underbrace{\Rightarrow}_{[6.12, \text{pg.84}]} \mathcal{I}(K, L) \subseteq \mathcal{I}(K, K^{\mathcal{I}(K,L)}) = I \Rightarrow |I| \geq |\mathcal{I}(K, L)| \underbrace{=}_{(1)} m \quad (1.1)$$

$$(1.1), (3) \Rightarrow |I| = m$$

$$\begin{cases} L \preceq K^{\mathcal{I}(K,L)} \preceq K \\ [K : L] = m \\ [K : K^{\mathcal{I}(K,L)}] \underbrace{=}_{(2.1)} m \end{cases} \underbrace{\Rightarrow}_{[2.18, \text{pg.16}]} [K^{\mathcal{I}(K,L)} : L] = 1 \Rightarrow L = K^{\mathcal{I}(K,L)}$$

□

Corollary 6.14. *Sia $F \preceq K$ separabile e finita, allora*

$$\left| \{L \mid F \preceq L \preceq K\} \right| \leq \left| \{T \mid T \subseteq \mathcal{I}(K, F)\} \right|$$

In particolare, una funzione iniettiva e'

$$f(L) = \mathcal{I}(K, L)$$

Proof: Siano A, B i due insiemi della tesi. f e' ben definita, infatti,

$$L \in A \Rightarrow F \preceq L \preceq K \underbrace{\Rightarrow}_{[6.5, \text{pg.79}]} \mathcal{I}(K, L) \subseteq \mathcal{I}(K, F) \Rightarrow \mathcal{I}(K, L) \in B$$

Sia $g : B \longrightarrow A$, la seguente funzione:

$$g(T) = K^T$$

E' anch'essa ben definita:

$$T \in B \Rightarrow T \subseteq \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.12, \text{pg.84}]} \quad F \preceq K^T \preceq K \Rightarrow K^T \in A$$

Infine, $gf = \text{id}_A$, infatti

$$gf(L) = g(\mathcal{I}(K, L)) = K^{\mathcal{I}(K, L)} \quad \underbrace{=}_{F \preceq K \text{ sep. e finita, [6.13, pg.86]}} \quad L$$

Quindi f e' iniettiva. □

Proposition 6.15.

$$F \preceq K \text{ finita e normale} \Rightarrow \mathcal{G}(K, F) = \mathcal{I}(K, F)$$

Proof: Per la prop [6.4, pg.79], sappiamo gia' che $\mathcal{G}(K, F) \subseteq \mathcal{I}(K, F)$. Resta da dimostrare $\supseteq$.

Sia $\varphi \in \mathcal{I}(K, F)$

$$F \preceq K \text{ finita} \quad \underbrace{\Rightarrow}_{[2.44, \text{pg.31}]} \quad K = F(\alpha_1, \dots, \alpha_n), \quad \alpha_i \in K \quad \forall i$$

$$\beta \in K \quad \underbrace{\Rightarrow}_{[2.21, \text{pg.18}]} \quad \beta = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}, \quad f, g \in F[x_1, \dots, x_n]$$

$$\varphi(\beta) \quad \underbrace{=}_{\varphi \text{ omomorfismo}} \quad \frac{\varphi f(\alpha_1, \dots, \alpha_n)}{\varphi g(\alpha_1, \dots, \alpha_n)} \quad \underbrace{=}_{\varphi|_F = \text{id}, f, g \in F[x_1, \dots, x_n]} \quad \frac{f(\varphi(\alpha_1), \dots, \varphi(\alpha_n))}{g(\varphi(\alpha_1), \dots, \varphi(\alpha_n))}$$

$$\Rightarrow \text{Im } \varphi = \left\{ \frac{f(\varphi(\alpha_1), \dots, \varphi(\alpha_n))}{g(\varphi(\alpha_1), \dots, \varphi(\alpha_n))} \mid f, g \in F[x_1, \dots, x_n], \quad g(\alpha_1, \dots, \alpha_n) \neq 0 \right\} \quad (1)$$

$$F \preceq K \text{ finita} \Rightarrow F \preceq K \text{ algebrica} \Rightarrow \alpha_i \text{ algebrico su } F \quad \forall i$$

$$\text{Sia } p_i(x) = P_{\min}(\alpha_i, F)$$

$$\varphi \in \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.6, \text{pg.80}]} \quad \varphi(\alpha_i) \text{ e' radice di } p_i(x)$$

$$\begin{cases} p_i(\alpha_i) = 0, \quad \alpha_i \in K \\ p_i(\varphi(\alpha_i)) = 0 \\ p_i(x) \text{ irrid. in } F[x] \\ F \preceq K \text{ e' normale} \end{cases} \Rightarrow \varphi(\alpha_i) \in K$$

$$\varphi(\alpha_i) \in K \quad \forall i \quad \underbrace{\Rightarrow}_{(1)} \quad \text{Im } \varphi \subseteq K \quad (2)$$

$$\varphi \in \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.3, \text{pg.78}]} \quad \varphi : K_F \longrightarrow \overline{F}_F \text{ e' una applicazione lineare iniettiva}$$

$$\Rightarrow K \quad \underbrace{\simeq}_{\text{isom. vettoriale}} \quad \varphi(K) \Rightarrow [\varphi(K) : F] = [K : F]$$

$$\begin{cases} (2) \Rightarrow \varphi(K) \subseteq K \\ [\varphi(K) : F] = [K : F] \end{cases} \quad \underbrace{\Rightarrow}_{[AL, 4.10.2, \text{pg.27}]} \quad \varphi(K) = K$$

Quindi, ricapitolando,

$$\begin{aligned}\varphi \text{ iniettiva} &\Rightarrow \varphi : K \longrightarrow \varphi(K) \text{ isomorfismo} \\ \varphi(K) = K &\Rightarrow \varphi : K \longrightarrow K \\ \varphi|_F = \text{id} \\ &\Rightarrow \varphi \in \mathcal{G}(K, F)\end{aligned}$$

□

Example 6.16.

$$\begin{aligned}\mathcal{G}(\mathbb{Q}(i), \mathbb{Q}) &= \mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) = \{\text{id}, f\} \\ \text{con } f(a + ib) &= a - ib\end{aligned}$$

Proof:

$$\begin{aligned}\mathbb{Q}(i) = CS(x^2 + 1, \mathbb{Q}) &\xRightarrow{\substack{[5.5, \text{pg. } 76]}} \mathbb{Q} \subseteq \mathbb{Q}(i) \text{ e' normale e finita} \xRightarrow{\substack{[6.15, \text{pg. } 87]}} \mathcal{G}(\mathbb{Q}(i), \mathbb{Q}) = \mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) = \\ &\xRightarrow{\substack{[6.2, \text{pg. } 78]}} \mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) = \{\text{id}, f\} \\ \text{con } f(a + ib) &= a - ib\end{aligned}$$

□

Proposition 6.17. Sia $F \preceq K$, $\alpha \in K$ e $H \leq G = \mathcal{G}(K, F)$ sottogruppo. Supponendo che

$$\begin{aligned}F \preceq K &\text{ estensione finita} \\ K^H &= F\end{aligned}$$

si ha

$$\begin{aligned}H &= \{\varphi_1, \dots, \varphi_s\} \\ \text{con } s < \infty, \quad \varphi_i &\neq \varphi_j \quad \forall i \neq j \\ P_{\min}(\alpha, F) &= \prod_{i=1}^r (x - \alpha_i) \\ \text{dove abbiamo posto} \\ \alpha'_i &= \varphi_i(\alpha) \in K \quad \forall i = 1, \dots, s \\ \{\alpha_1, \dots, \alpha_r\} &= \{\alpha'_1, \dots, \alpha'_s\} \\ \text{con } r \leq s, \quad \alpha_i &\neq \alpha_j \quad \forall i \neq j\end{aligned}$$

In particolare, la tesi vale per $H = G$.

Proof: Osserviamo che

$$F \preceq K \text{ finita} \Rightarrow |G| \leq [K : F] < +\infty$$

[6.10, pg. 84]

$$H \subseteq G \Rightarrow |H| \leq |G| < +\infty$$

Quindi, possiamo scrivere $H = \{\varphi_1, \dots, \varphi_s\}$ con $\varphi_i \neq \varphi_j \quad \forall i \neq j$.

Sia $\alpha \in K$, e siano

$$\begin{aligned}\alpha'_i &= \varphi_i(\alpha) \in K \quad \forall i = 1, \dots, s \\ \{\alpha_1, \dots, \alpha_r\} &= \{\alpha'_1, \dots, \alpha'_s\} \\ \text{con } r \leq s, \quad \alpha_i &\neq \alpha_j \quad \forall i \neq j\end{aligned}$$

Sia

$$h(x) = \prod_{i=1}^r (x - \alpha_i) \in K[x]$$

(1) Dim. $h(x) = P_{\min}(\alpha, F)$

Sia $\varphi \in H$, e sia $A = \{\alpha_1, \dots, \alpha_r\}$

(1.1) Dim. $\varphi|_A : A \longrightarrow A$ e' una biezione, ovvero e' una permutazione su A

Per costruzione $\forall \alpha_i \exists i' : \alpha_i = \varphi_{i'}(\alpha)$

$$\varphi(\alpha_i) = \varphi(\varphi_{i'}(\alpha)) = \varphi \circ \varphi_{i'}(\alpha) \underset{H \text{ e' un gruppo}}{=} \varphi_{j'}(\alpha) = \alpha_{j'} \in A$$

$$\Rightarrow \varphi|_A(A) \subseteq A \quad (*)$$

$$\varphi \in H \subseteq G = \mathcal{G}(K, F) \Rightarrow \varphi \text{ e' iniettiva} \quad (**)$$

$$\begin{cases} |A| < \infty \\ (*), (**) \end{cases} \Rightarrow \varphi \text{ surriettiva}$$

(1.2) $h(x) \in F[x]$

$h(x)$ e' per costruzione simmetrico nelle variabili $\alpha_1, \dots, \alpha_r$, quindi non cambia applicandogli l'indotto Φ_i della permutazione $\varphi_{i|_A}$:

$$\Phi_i(h) = h$$

o piu' in dettaglio:

$$h(x) = a_0 + a_1x + \dots + a_rx^r$$

$$\Phi_i(h)(x) = \varphi_i(a_0) + \varphi_i(a_1)x + \dots + \varphi_i(a_r)x^r =$$

$$\underset{\varphi_i \text{ omomorfismo}}{=} \prod_{j=1}^r (x - \varphi_i(\alpha_j)) \underset{\varphi_i \text{ permuta gli } \alpha_j}{=} h(x) = a_0 + a_1x + \dots + a_rx^r$$

$$a_0 + a_1x + \dots + a_rx^r = \varphi_i(a_0) + \varphi_i(a_1)x + \dots + \varphi_i(a_r)x^r \Leftrightarrow \begin{cases} \varphi_i(a_0) = a_0 \\ \varphi_i(a_1) = a_1 \\ \dots \\ \varphi_i(a_r) = a_r \end{cases} \Leftrightarrow \varphi_i(a_j) = a_j \quad \forall j = 1, \dots, r$$

$$\varphi_i(a_j) = a_j \quad \forall i = 1, \dots, s \Leftrightarrow \varphi(a_j) = a_j \quad \forall \varphi \in H \Rightarrow a_j \in K^H$$

$$a_j \in K^H \quad \forall j \Rightarrow h(x) \in K^H[x] \underset{K^H=F}{=} F[x]$$

Sia $p(x) = P_{\min}(\alpha, F)$

(1.3) $h(x) = p(x)$

Sempre per costruzione $h(\alpha_i) = 0 \quad \forall i$, cioè

$$h(\varphi_{i'}(\alpha)) = 0 \quad \forall i$$

$$\varphi_{i'} \in H \subseteq G \subseteq \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.7, \text{pg.80}]} p(\varphi_{i'}(\alpha)) = 0 \Leftrightarrow p(\alpha_i) = 0 \Rightarrow x - \alpha_i \not\mid p(x)$$

$$x - \alpha_i \not\mid p(x) \quad \forall i = 1, \dots, r \Rightarrow h(x) \not\mid p(x)$$

$$\alpha = \text{id}(\alpha), \text{id} \in H \Rightarrow \exists k : \alpha = \alpha_k$$

$$\begin{cases} h(x) \underbrace{\in}_{\text{passo 1.2}} F[x] \\ h(\alpha) = h(\alpha_k) = 0 \end{cases} \quad \underbrace{\Rightarrow}_{[2.28, \text{pg.23}]} p(x) \not\mid h(x)$$

$$\begin{cases} h(x) \not\mid p(x) \\ p(x) \not\mid h(x) \end{cases} \Rightarrow p(x) = h(x)$$

□

Lemma 6.18.

$$\begin{cases} F \preceq K \text{ algebrica} \\ K = F(\alpha_1, \dots, \alpha_n) \\ \alpha_1, \dots, \alpha_n \in K, \text{ separabili su } F \end{cases} \Rightarrow \exists \gamma \in K \text{ separabile su } F \text{ t.c. } K = F(\gamma)$$

*Nota*¹⁹

Proof: Sfruttiamo la dimostrazione del thm [3.29,pg.65]. Osserviamo intanto che le ipotesi garantiscono la (1) e (2) della dim di [3.29,pg.65].

(1) Supponiamo F finito

Ripetendo la dimostrazione di [3.29,pg.65], nel caso finito, abbiamo

$$F \preceq K \text{ finita, } K \text{ finito}$$

$$\exists \alpha \in K \quad K = F(\alpha)$$

Infine,

$$\begin{cases} F \text{ finito} \\ F \preceq K \text{ algebrica} \end{cases} \quad \underbrace{\Rightarrow}_{[3.27, \text{pg.62}]} F \preceq K \text{ separabile} \Rightarrow \alpha \text{ separabile}$$

(2) Supponiamo F infinito

Procediamo per induzione su n

(2.1) $n = 1$

$$K = F(\alpha_1), \quad \alpha_1 \text{ separabile}$$

(2.2) $n = 2$

Poniamo

$$\alpha = \alpha_1, \quad \beta = \beta_1$$

$$f(x) = P_{\min}(\alpha, F), \quad g(x) = P_{\min}(\beta, F)$$

$$\alpha_1, \alpha_2, \dots, \alpha_r \text{ tutte le radici di } f(x)$$

$$\beta_1, \beta_2, \dots, \beta_s \text{ tutte le radici di } g(x)$$

¹⁹a differenza del thm [3.29,pg.65], stiamo affermando che γ e' separabile e non stiamo richiedendo che $F \preceq K$ sia separabile.

Poiche' F e' infinito

$$\exists \lambda \in F : \lambda \neq \frac{\alpha_h - \alpha_i}{\beta_j - \beta_q} \begin{cases} 1 \leq h, i \leq r \\ 1 \leq j \neq q \leq s \end{cases} \quad (1)$$

$$\Rightarrow \alpha_i + \lambda \beta_j \neq \alpha_h + \lambda \beta_q \quad \forall j \neq q \quad (1.1)$$

Inoltre,

$$\alpha \text{ separabile} \Rightarrow P_{\min}(\alpha, F) = f(x) \text{ separabile} \Rightarrow \alpha_1, \alpha_2, \dots, \alpha_r \text{ sono distinte} \Rightarrow \alpha_i + \lambda \beta_j \neq \alpha_h + \lambda \beta_j \quad \forall i \neq h$$

$$\underbrace{\Rightarrow \alpha_i + \lambda \beta_j \neq \alpha_h + \lambda \beta_q \quad \forall i \neq h}_{(1.1)} \quad (1.2)$$

$$\alpha_i + \lambda \beta_j = \alpha_h + \lambda \beta_q \quad \underbrace{\Leftrightarrow}_{(1.1), (1.2)} i = h \wedge h = q \quad (1.3)$$

Riusando la dimostrazione del thm [3.29,pg.65] nel caso $n = 2$, otteniamo
 $K = F(\alpha + \lambda \beta)$

Nota²⁰ Sia $\gamma = \alpha + \lambda \beta$.

(2.2.1) Dimostriamo che γ e' separabile su F

Sia

$$s(x) = \prod_{j=1}^s f(x - \lambda \beta_j)$$

$$(2.2.1.1) \quad s(\gamma) = 0$$

$$s(\alpha + \lambda \beta) = f(\alpha + \lambda \beta - \lambda \beta_1) f(\alpha + \lambda \beta - \lambda \beta_2) \dots$$

$$f(\alpha + \lambda \beta - \lambda \beta_1) \underbrace{=}_{\beta_1 = \beta} f(\alpha) = 0$$

(2.2.1.2) $s(x)$ e' separabile

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_r)$$

$$f(x - \lambda \beta_j) = \prod_{i=1}^r (x - (\alpha_i + \lambda \beta_j))$$

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

$$\Rightarrow \text{le radici di } s(x) \text{ sono } \alpha_i + \lambda \beta_j \underbrace{\Rightarrow}_{(1.3)} \text{ sono tutte distinte} \Rightarrow s(x) \text{ e' separabile}$$

$$(2.2.1.3) \quad s(x) \in F[x]$$

Poniamo

$$S(x_1, \dots, x_s, x) = \prod_{j=1}^s f(x - \lambda x_j) \in F[x_1, \dots, x_s, x]$$

dove $x_1, \dots, x_s, x$ sono delle indeterminate. Si ha

$$\begin{cases} S \text{ e' simmetrico nella variabili } x_1, \dots, x_s \\ S(x_1, \dots, x_s, x) = \sum_{i=1}^{rs} q_i(x_1, \dots, x_s) x^i \end{cases} \quad q_i \text{ sono simmetrici} \quad \underbrace{\Rightarrow}_{[5.1, \text{pg.74}]} q_i(\beta_1, \dots, \beta_s) \in F[x] \quad \forall i$$

$$\Rightarrow s(x) = S(\beta_1, \dots, \beta_s, x) \in F[x]$$

²⁰la dimostrazione del thm [3.29,pg.65] nel caso $n = 2$ funziona anche supponendo che α, β siano separabili, senza richiedere che $F \preceq K$ sia separabile.

Sia $p(x) = P_{\min}(\alpha, F)$

$$\begin{cases} s(x) \in F[x] \\ s(\alpha) = 0 \end{cases} \xRightarrow{[2.28, \text{pg.23}]} p(x)/s(x)$$

$$\begin{cases} p(x)/s(x) \\ s(x) \text{ separabile} \end{cases} \xRightarrow{[3.19, \text{pg.58}]} p(x) \text{ separabile}$$

(2.3) $n - 1 \Rightarrow n$

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \xRightarrow{\text{Hp induttiva}} F(\gamma_1)(\alpha_n), \quad \gamma_1 \text{ separabile su } F$$

$$\gamma_1, \alpha_n \text{ separabili su } F \xRightarrow{\text{passo 2.2}} F(\gamma_1, \alpha_n) = F(\gamma_2) \quad \gamma_2 \text{ separabile.}$$

□

Theorem 6.19. Data $F \preceq K$ finita, le seguenti proposizioni sono equivalenti:

1. $F \preceq K$ e' normale e separabile
2. $\exists f(x) \in F[x]$ separabile t.c. $K = CS(f(x), F)$

in particolare, se $K = F(\alpha_1, \dots, \alpha_n)$, α_i algebrico, un tale f e' $f(x) = \prod \{P_{\min}(\alpha_i, F) \mid i = 1, \dots, n\}$

3. $F \preceq L \preceq K \Rightarrow |\mathcal{G}(K, L)| = [K : L]$
4. $F = K^{\mathcal{G}(K, F)}$
5. $|\mathcal{G}(K, F)| = [K : F]$

Proof:

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

Si ha

$$F \preceq K \text{ finita} \xRightarrow{[2.44, \text{pg.31}]} K = F(\alpha_1, \dots, \alpha_n), \quad \alpha_i \text{ algebrico} \quad \forall i$$

Sia $p_i(x) = P_{\min}(\alpha_i, F) \quad \forall i = 1, \dots, n$

$$F \preceq K \text{ normale, finita} \xRightarrow{[5.5, \text{pg.76}]} K = CS\left(\prod_{i=1}^n p_i(x), F\right) \quad (1)$$

Siano dati $q_i(x) \quad \forall i, \dots, r$ tali che

$$\begin{cases} \{q_i(x) \mid i = 1, \dots, r\} = \{p_i(x) \mid i = 1, \dots, n\} \\ q_i(x) \neq q_j(x) \quad \forall i \neq j \\ r \leq n \end{cases} \quad (2)$$

si ha

$$\prod_{i=1}^n p_i(x) \xRightarrow{\text{alcuni } p_i(x) \text{ potrebbero essere uguali}} \prod_{i=1}^r q_i(x)^{e_i} \xRightarrow{\text{spezzando i } q_i(x)} \prod_{i=1}^r \prod_{j=1}^{n_i} (x - \alpha_{ij})^{e_i} \quad (1.0)$$

dove $\alpha_{i1}, \dots, \alpha_{in_i}$ sono le radici di $q_i(x)$ e quindi, per la (2), sono le radici di qualche $p_j(x)$

$\alpha_{ij} \quad \forall i, j$ sono tutte le radici dei vari $q_i(x)$ e quindi anche dei vari $p_j(x)$

$$(1) \Rightarrow K = F(\alpha_{ij}, \quad \forall i, j) \quad (1.1)$$

Sia $f(x) = \prod_{i=1}^r q_i(x)$, si ha

$$\begin{aligned} f(x) &= \prod_{i=1}^r q_i(x) \underbrace{=}_{(1.0)} \prod_{i=1}^r \prod_{j=1}^{n_i} (x - \alpha_{ij}) \quad (1.2) \\ &\Rightarrow CS(f(x), F) = F(\alpha_{ij}, \forall i, j) \underbrace{=}_{(1.1)} K \end{aligned}$$

Resta da dimostrare che $f(x)$ e' separabile.

$$F \preceq K \text{ separabile} \Rightarrow \alpha_i \text{ separabile } \forall i \Rightarrow p_i(x) \text{ separabile } \forall i \Rightarrow q_i(x) \text{ separabile } \forall i \Rightarrow \alpha_{ij} \neq \alpha_{ik} \quad \forall j \neq k \quad (3)$$

Se per assurdo, $\exists i \neq h, j, k : \alpha_{ij} = \alpha_{hk}$, con allora

$$\begin{cases} q_h(\alpha_{hk}) = 0 = q_i(\alpha_{ij}) \\ q_h, q_i \text{ monico} \\ q_h, q_i \text{ irriducibile in } F[x] \end{cases} \Rightarrow \begin{cases} q_h(x) = P_{\min}(\alpha_{hk}, F) \\ q_i(x) = P_{\min}(\alpha_{ij}, F) \end{cases} \underbrace{\Rightarrow}_{\alpha_{ij}=\alpha_{hk}} \Rightarrow q_h(x) = q_i(x) \underbrace{\Rightarrow}_{(2)} i = h \text{ assurdo} \quad (4)$$

Quindi

$$i \neq h \Rightarrow \alpha_{ij} \neq \alpha_{hk} \quad (4.1)$$

$$(4.1), (3) \Rightarrow \alpha_{ij} \neq \alpha_{hk} \quad \forall i \neq h \vee j \neq k$$

$$\alpha_{ij} = \alpha_{hk} \Leftrightarrow i = h, j = k$$

quindi tutte le α_{ij} sono tra loro distinte, e quindi dalla (1.2) $f(x)$ e' separabile.

(2) Dim 2. $\Rightarrow$ 3.

Per la 2. abbiamo

$$K = CS(f(x), F), \quad f(x) \in F[x] \quad (1)$$

$$f(x) \text{ separabile} \quad (1.1)$$

Siano $\alpha_1, \dots, \alpha_n \in K$ tutte le radici di $f(x)$. Si ha

$$\begin{cases} K = CS(f(x), F) \\ F \preceq L \preceq K \end{cases} \underbrace{\Rightarrow}_{[2.54, \text{pg.} 42]} K = CS(f(x), L)$$

Abbiamo

$$K = CS(f(x), L) \underbrace{\Rightarrow}_{[5.5, \text{pg.} 76]} L \preceq K \text{ e' normale, finita} \underbrace{\Rightarrow}_{[6.15, \text{pg.} 87]} \mathcal{G}(K, L) = \mathcal{I}(K, L) \Rightarrow |\mathcal{G}(K, L)| = |\mathcal{I}(K, L)| \quad (2)$$

$$f(\alpha_i) = 0, \quad f(x) \in F[x] \subseteq L[x] \underbrace{\Rightarrow}_{[2.28, \text{pg.} 23]} p_i(x) = P_{\min}(\alpha_i, L) / f(x)$$

$$\begin{cases} p_i(x) / f(x) \\ (1) \Rightarrow f(x) \text{ separabile} \end{cases} \underbrace{\Rightarrow}_{[3.19, \text{pg.} 58]} p_i(x) \text{ separabile} \underbrace{\Rightarrow}_{\text{per def.}} \alpha_i \text{ separabile su } L$$

$$L \preceq K \text{ finita} \underbrace{\Rightarrow}_{[2.44, \text{pg.} 31]} L \preceq K \text{ algebrica}$$

$$\begin{cases} L \preceq K \text{ algebrica} \\ \alpha_i \text{ separabile su } L \quad \forall i \\ K = CS(f(x), L) = L(\alpha_1, \dots, \alpha_n) \end{cases} \underbrace{\Rightarrow}_{[6.18, \text{pg.} 90]} \exists \gamma \in K \text{ separabile su } L \text{ t.c. } K = L(\gamma) \quad (3)$$

γ separabile su $L \Rightarrow p(x) = P_{\min}(\gamma, L)$ separabile $\Rightarrow (\gamma_1 = \gamma), \dots, \gamma_r$ radici di $p(x)$ sono distinte $\Rightarrow$

$$\Rightarrow r = |\{\gamma_1, \dots, \gamma_r\}| \underbrace{=}_{\text{applicando [6.8, pg. 81] con } \varphi = \text{id}} |\mathcal{I}(K, L)| \underbrace{=}_{(2)} |\mathcal{G}(K, L)|$$

$$|\mathcal{G}(K, L)| = r = \deg p(x) \underbrace{=}_{[2.40, \text{pg.} 29]} [L(\gamma) : L] \underbrace{=}_{(3)} [K : L]$$

$$|\mathcal{G}(K, L)| = [K : L]$$

(3) Dim 3. $\Rightarrow$ 4.

Sia $G = \mathcal{G}(K, F)$,

$$\begin{cases} F \preceq K \text{ algebrica} \\ G \underset{[6.4, \text{pg.79}]}{\subseteq} \mathcal{I}(K, F) \underset{[6.12, \text{pg.84}]}{\Rightarrow} F \preceq K^G \preceq K \end{cases} \quad (1)$$

$$(1), F \preceq K \text{ finita} \underset{[2.18, \text{pg.16}]}{\Rightarrow} [K : K^G][K^G : F] = [K : F] \quad (2)$$

$$\Rightarrow l = [K : K^G] \leq [K : F] = m \quad (2.2)$$

$$l = [K : K^G] \underset{3. \text{ con } L=K^G}{=} |\mathcal{G}(K, K^G)| \underset{[6.12, \text{pg.84}]}{\geq} |G| \underset{3. \text{ con } L=F}{=} [K : F] = m$$

$$\Rightarrow l \geq m \quad (3)$$

$$(2.2), (3) \Rightarrow l = m \underset{(2)}{\Rightarrow} [K^G : F] = 1 \Rightarrow F = K^G$$

(4) 4. $\Rightarrow$ 1.

Sia $G = \mathcal{G}(K, F)$, $\alpha \in K$, $h(x) = P_{\min}(\alpha, F)$, si ha

(4.1) $h(x) = \prod_{i=1}^r (x - \alpha_i)$, con $\alpha_1, \dots, \alpha_r \in K$ distinti fra loro

$$\begin{cases} F \preceq K \text{ finita} \\ K^G \underset{4.}{=} F \end{cases} \underset{[6.17, \text{pg.88}]}{\Rightarrow} \begin{cases} G = \{\varphi_1, \dots, \varphi_s\} \\ h(x) = P_{\min}(\alpha, F) = \prod_{i=1}^r (x - \alpha_i) \end{cases} \quad \text{dove}$$

$$\alpha'_i = \varphi_i(\alpha) \in K \quad \forall i = 1, \dots, s$$

$$\{\alpha_1, \dots, \alpha_r\} = \{\alpha'_1, \dots, \alpha'_s\}$$

$$\text{con } r \leq s, \quad \alpha_i \neq \alpha_j \quad \forall i \neq j$$

(4.2) $F \preceq K$ e' separabile

Sia $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$. Per passo 4.1 abbiamo che

$$\exists \alpha_1, \dots, \alpha_r \in K : p(x) = \prod_{i=1}^r (x - \alpha_i), \quad \alpha_i \neq \alpha_j \quad \forall i \neq j$$

quindi $p(x)$ e' separabile

(4.3) $F \preceq K$ e' normale

Sia $\bar{f}(x) \in F[x]$ irriducibile, $\bar{f}(x) = af(x)$, $f(x)$ monico, e supponiamo $\exists \alpha \in K : f(\alpha) = 0$.

Sempre per

$$\begin{cases} f(x) \in F[x] \text{ irriducibile} \\ f(\alpha) = 0 \\ f(x) \text{ monico} \end{cases} \underset{[2.30, \text{pg.24}]}{\Rightarrow} f(x) = P_{\min}(\alpha, F) \underset{\text{passo 4.1}}{=} \prod_{i=1}^r (x - \alpha_i), \quad \alpha_i \in K \quad \forall i$$

Quindi $f(x)$ ha tutte le radici in K .

Per l'arbitrarieta' di $f(x)$ deduciamo che $F \preceq K$ e' normale.

(5) 3. $\Rightarrow$ 5.

Basta scegliere $L = F$

(6) 5. $\Rightarrow$ 4.

Sia $G = \mathcal{G}(K, F)$, $F' = K^G$.

$$G \subseteq \mathcal{I}(K, F) \xRightarrow{[6.12, \text{pg.84}]} F \preceq K^G = F' \preceq K$$

$$F \preceq K \text{ finita} \xRightarrow{[2.18, \text{pg.16}]} F' \preceq K \text{ finita}, [K : F] = [K : F'] [F' : F] \quad (*)$$

Possiamo perciò applicare le proposizioni fin'ora dimostrate alla estensione $F' \preceq K$.

$$\mathcal{G}(K, F') = \mathcal{G}(K, K^G) \xRightarrow{[6.12, \text{pg.84}]} = G \quad (1)$$

$$\begin{aligned} K^{\mathcal{G}(K, F')} &\xRightarrow{(1)} K^G = F' \xRightarrow{4. \Rightarrow 3.} |\mathcal{G}(K, F')| = [K : F'] \quad (2) \quad [K : F] \xRightarrow{5.} |\mathcal{G}(K, F)| \xRightarrow{[6.12, \text{pg.84}]} |\mathcal{G}(K, K^{\mathcal{G}(K, F)})| = \\ &= |\mathcal{G}(K, K^G)| \xRightarrow{(2)} [K : F'] \end{aligned}$$

$$[K : F] = [K : F'] \xRightarrow{(*)} [F' : F] = 1 \Rightarrow F' = F \Leftrightarrow K^G = F$$

□

Definition 6.20. Sia $F \preceq K$ una estensione finita.

$F \preceq K$ e' una estensione di Galois $\stackrel{\text{def}}{\Leftrightarrow}$ vale una qualsiasi prop. del thm [6.19,pg.92]

Example 6.21.

$$\begin{aligned} \mathbb{Q} &\subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \mathbb{Q} &\subseteq \mathbb{Q}(\omega, \sqrt[3]{2}) \end{aligned}$$

sono estensioni di Galois.

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$$

non e' di Galois.

Proof:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = CS(p(x), \mathbb{Q}) \quad (*)$$

$$p(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$$

$$p(x) = (x - (\sqrt{2} + \sqrt{3}))(x + (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x + (\sqrt{2} - \sqrt{3})) \Rightarrow p(x) \text{ e' separabile} \quad (**)$$

$$(*), (**) \xRightarrow{2. \text{ di } [6.19, \text{pg.92}]} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \text{ e' di Galois}$$

$$\mathbb{Q}(\omega, \sqrt[3]{2}) = CS(x^3 - 2, \mathbb{Q}[x])$$

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2) \Rightarrow x^3 - 2 \text{ e' separabile}$$

$$\xRightarrow{2. \text{ di } [6.19, \text{pg.92}]} \mathbb{Q} \subseteq \mathbb{Q}(\omega, \sqrt[3]{2}) \text{ e' di Galois}$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \text{ non e' normale (vedi [5.4,pg.76])} \xRightarrow{1. \text{ di } [6.19, \text{pg.92}]} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \text{ non e' di Galois}$$

□

Proposition 6.22. Sia $F \preceq K$, $f(x) \in F[x]$, si ha

$$\begin{cases} \text{ch}F = 0 \\ K = CS(f(x), F) \end{cases} \Rightarrow F \preceq K \text{ e' di Galois}$$

In pratica, se $\text{ch}F = 0$, la separabilita' di f non e' piu' necessaria.

Proof:

$$K = CS(f(x), F) \xRightarrow{[5.5, \text{pg.76}]} F \preceq K \text{ e' normale e finita}$$

$$F \preceq K \text{ finita} \Rightarrow F \preceq K \text{ algebrica}$$

$$\begin{cases} F \preceq K \text{ algebrica} \\ \text{ch}F = 0 \end{cases} \xRightarrow{[3.23, \text{pg.60}]} F \preceq K \text{ e' separabile}$$

$$F \preceq K \text{ e' finita, normale, separabile} \xRightarrow{[6.19, \text{pg.92}]} F \preceq K \text{ e' di Galois}$$

□

Proposition 6.23.

$$\begin{cases} F \preceq K \text{ e' di Galois} \\ F \preceq L \preceq K \end{cases} \Rightarrow L \preceq K \text{ e' di Galois, ma non e' detto che pure } F \preceq L \text{ lo sia}$$

Proof:

$$F \preceq K \text{ e' di Galois} \xRightarrow{[6.19, \text{pg.92}]} K = CS(f(x), F), \text{ } f(x) \text{ separabile}$$

$$\begin{cases} K = CS(f(x), F) \\ F \preceq L \preceq K \end{cases} \xRightarrow{[2.54, \text{pg.42}]} K = CS(f(x), L)$$

$$\begin{cases} K = CS(f(x), L) \\ f(x) \text{ separabile} \end{cases} \xRightarrow{[6.19, \text{pg.92}]} L \preceq K \text{ e' di Galois}$$

Non e' detto che $F \preceq L$ sia di Galois, infatti, l'esempio [6.21, pg.95] mostra che

$$\underbrace{\mathbb{Q}}_F \subseteq \underbrace{\mathbb{Q}(\sqrt[3]{2})}_L \subseteq \underbrace{\mathbb{Q}(\omega, \sqrt[3]{2})}_K$$

$F \preceq K$ e' di Galois, ma $F \preceq L$ non lo e'

□

Proposition 6.24. Sia $F \preceq K$ una estensione di Galois. Si ha

$$\mathcal{G}(K, F) = \mathcal{I}(K, F)$$

Proof:

$$F \preceq K \text{ di Galois} \xRightarrow{[6.19, \text{pg.92}]} F \preceq K \text{ finita, normale, separabile} \xRightarrow{[6.15, \text{pg.87}]} \mathcal{G}(K, F) = \mathcal{I}(K, F)$$

□

Theorem 6.25. *Corrispondenza di Galois.*

Sia $F \preceq K$ una estensione di Galois, allora

$$\left| \{L \mid F \preceq L \preceq K\} \right| = \left| \{H \mid H \leq \mathcal{G}(K, F) \text{ sottogruppo}\} \right|$$

In particolare, un funzione biettiva tra i due insiemi e'

$$f(L) = \mathcal{G}(K, L)$$

$$f^{-1}(H) = K^H$$

Proof:

(1) f e' ben definita

$$F \preceq L \preceq K \xRightarrow{\text{[6.4,pg.79]}} \mathcal{G}(K, L) \leq \mathcal{G}(K, F)$$

(2) f e' iniettiva

Sfruttiamo quello che abbiamo gia' visto nella prop. [6.14,pg.86], considerando anche la prop [6.24,pg.96]

$$F \preceq K \text{ di Galois} \xRightarrow{\text{[6.19,pg.92]}} F \preceq K \text{ finita, normale, separabile} \Rightarrow$$

$$\xRightarrow{\text{[6.14,pg.86]}} \begin{cases} \varphi : \{L \mid F \preceq L \preceq K\} \longrightarrow \{T \mid T \subseteq \mathcal{I}(K, F)\} \\ \varphi(L) = \mathcal{I}(K, L) \end{cases} \quad \text{e' un funzione iniettiva (*)}$$

$$\begin{cases} F \preceq K \text{ di Galois} \\ F \preceq L \preceq K \end{cases} \xRightarrow{\text{[6.23,pg.96]}} L \preceq K \text{ di Galois} \xRightarrow{\text{[6.24,pg.96]}} \mathcal{G}(K, L) = \mathcal{I}(K, L)$$

$$\varphi(L) = \mathcal{I}(K, L) = \mathcal{G}(K, L) = f(L) \quad \forall L \Rightarrow f = \varphi \xRightarrow{(*)} f \text{ iniettiva}$$

(3) f e' surriettiva

Consideriamo la funzione

$$g : \{H \leq \mathcal{G}(K, F)\} \longrightarrow \{L \mid L \preceq F \preceq K\}$$

$$g(H) = K^H$$

E' anch'essa ben definita:

$$H \leq \mathcal{G}(K, F) \xRightarrow{\text{[6.12,pg.84]}} F \preceq K^H \preceq K$$

Per dimostrare che f e' surriettiva, proviamo che $fg = \text{id}$, ovvero che

$$fg(H) = f(K^H) = \mathcal{G}(K, K^H) = H$$

(3.1) Dim. $\mathcal{G}(K, K^H) = H$

Sia $F' = K^H$

(3.1.1) Dim. $H \subseteq \mathcal{G}(K, F')$

$$\begin{cases} F \preceq K \text{ di Galois} \\ F \preceq K^H \preceq K \end{cases} \xRightarrow{\text{[6.23,pg.96]}} K^H \preceq K \text{ di Galois} \quad (1)$$

$$\xRightarrow{\text{[6.24,pg.96]}} \mathcal{I}(K, K^H) = \mathcal{G}(K, K^H) \quad (2)$$

$$H \xRightarrow{\text{[6.12,pg.84]}} \mathcal{I}(K, K^H) \xRightarrow{(2)} \mathcal{G}(K, K^H) \quad (2.1)$$

Resta da dimostrare $H \supseteq \mathcal{G}(K, K^H)$.
 (3.1.2) Dim. che $|H| = [K : F']$

$$\begin{aligned}
 (1) \Rightarrow F' \preceq K \text{ di Galois} & \xRightarrow{\text{[6.19,pg.92]}} F' \preceq K \text{ finita, separabile} \quad (1.1) \\
 & \xRightarrow{\text{[2.44,pg.31]}} K = F'(\alpha_1, \dots, \alpha_n), \alpha_1, \dots, \alpha_n \text{ separabili, } F' \preceq K \text{ algebrica} \Rightarrow \\
 & \xRightarrow{\text{[6.18,pg.90]}} \exists \gamma \in K \text{ separabile su } F' \text{ t.c. } K = F'(\gamma) \quad (3)
 \end{aligned}$$

Poiche'

$$\begin{aligned}
 & \gamma \in K \\
 & H \xRightarrow{\text{passo 3.1.1}} \mathcal{G}(K, F')
 \end{aligned}$$

$$\begin{aligned}
 (1.1) \Rightarrow F' \preceq K \text{ estensione finita} \\
 F' = K^H
 \end{aligned}$$

per la prop [6.17,pg.88] si ha

$$\begin{aligned}
 H &= \{h_1, \dots, h_s\} \\
 &\text{con } s < \infty, \quad h_i \neq h_j \quad \forall i \neq j \quad (4)
 \end{aligned}$$

$$p(x) = P_{\min}(\gamma, F') = \prod_{i=1}^r (x - \gamma_i) \quad (4.0)$$

dove abbiamo posto

$$\begin{aligned}
 \gamma'_i &= h_i(\gamma) \in K \quad \forall i = 1, \dots, s \\
 \{\gamma_1, \dots, \gamma_r\} &= \{\gamma'_1, \dots, \gamma'_s\} \quad (4.1)
 \end{aligned}$$

$$\text{con } r \leq s, \quad \gamma_i \neq \gamma_j \quad \forall i \neq j \quad (4.2)$$

(3.1.2.1) $h_i(\gamma) \neq h_j(\gamma) \quad \forall i \neq j$

Per la (3) possiamo applicare il thm [6.8,pg.81] (con $\varphi = \text{id}$), e abbiamo

$$\begin{aligned}
 E = \mathcal{I}(K, F') & \xRightarrow{\text{[6.24,pg.96]}} \mathcal{G}(K, F')
 \end{aligned}$$

$$|E| = \left| \{g(\gamma) \mid g \in E\} \right|, \text{ con biezione } g \in E \mapsto g(\gamma) \quad (5)$$

$$\text{Presi } h_i, h_j \in H \xRightarrow{\text{passo 3.1.1}} \mathcal{G}(K, F') = E$$

$$h_i(\gamma) = h_j(\gamma) \xLeftrightarrow{(5)} h_i = h_j \xLeftrightarrow{(4)} i = j$$

$$\Rightarrow h_i(\gamma) \neq h_j(\gamma) \quad \forall i \neq j \quad (6)$$

Dalla (6), (4.1), (4.2) segue che, a meno di riordinare gli indici,

$$r = s, \quad \gamma_i = \gamma'_i \quad \forall i = 1, \dots, r$$

e quindi

$$\deg p(x) = r = s = |H|$$

$$\begin{aligned}
 p(x) = P_{\min}(\gamma, F') & \xRightarrow{\text{[2.40,pg.29]}} [F'(\gamma) : F'] = \deg p(x) = |H| \xLeftrightarrow{(3)} [K : F'] = |H|
 \end{aligned}$$

Per concludere,

$$\begin{aligned}
(1) \Rightarrow F' \preceq K \text{ di Galos} & \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} \left| \mathcal{G}(K, F') \right| = [K : F'] \underbrace{=}_{\text{passo 3.1.2}} |H| \underbrace{\leq}_{\text{passo 3.1.1}} \left| \mathcal{G}(K, F') \right| \Rightarrow |H| = \left| \mathcal{G}(K, F') \right| \\
\left| \mathcal{G}(K, F') \right| &= [K : F'] \underbrace{\leq}_{F' \preceq K \text{ e' finita}} \infty \\
\begin{cases} |H| = \left| \mathcal{G}(K, F') \right| < \infty \\ H \subseteq \mathcal{G}(K, F') \end{cases} & \Rightarrow H = \mathcal{G}(K, F') = \mathcal{G}(K, K^H)
\end{aligned}$$

□

Proposition 6.26. *Sia $f(x) \in F[x]$ separabile, $K = CS(f(x), F)$, $A = \{\alpha_1, \dots, \alpha_n\}$ l'insieme delle radici di $f(x)$, $\deg f(x) = n$. Si ha la seguente immersione tra gruppi:*

$$\begin{aligned}
\Phi : \mathcal{G}(K, F) &\hookrightarrow S_n(A) \\
\varphi &\mapsto \varphi|_A
\end{aligned}$$

dove $S_n(A)$ e' il gruppo delle permutazioni su A , che puo' essere visto direttamente come S_n .

Proof:

(1) Dim. che Φ e' ben posta.

Presa $\varphi \in \mathcal{G}(K, F)$ dimostriamo che $\varphi' = \varphi|_A \in S_n(A)$.

$$\begin{aligned}
\varphi'(\alpha_i) &\in A, \text{ infatti} \\
f(\varphi'(\alpha_i)) &= f(\varphi(\alpha_i)) \underbrace{=}_{[6.7, \text{pg.80}]} \varphi(f(\alpha_i)) = \varphi(0) = 0 \\
f(\varphi'(\alpha_i)) &= 0 \Rightarrow \varphi'(\alpha_i) \in A \\
\varphi \in \mathcal{G}(K, F) &\Rightarrow \varphi \text{ iniettiva} \Rightarrow \varphi' \text{ iniettiva} \\
\begin{cases} \varphi' : A \longrightarrow A \\ \varphi' \text{ iniettiva} \\ A \text{ finito} \end{cases} &\Rightarrow \varphi' \text{ biettiva} \\
f(x) \text{ separabile} &\Rightarrow \alpha_1, \dots, \alpha_n \text{ sono tutte distinte} \Rightarrow |A| = n \\
\begin{cases} \varphi' \text{ biettiva} \\ |A| = n \end{cases} &\Rightarrow \varphi' \in S_n(A)
\end{aligned}$$

(2) Dim. che Φ e' un omomorfismo tra gruppi

$$\begin{aligned}
\Phi(fg) &= (fg)|_A = fg|_A \\
g|_A \in S_n(A) &\Rightarrow \text{Im } g|_A = A \Rightarrow fg|_A = f|_A g|_A \\
\Phi(f) \circ \Phi(g) &= f|_A \circ g|_A = fg|_A = \Phi(fg)
\end{aligned}$$

(3) Φ e' iniettiva

$$\ker \Phi = \{f \in \mathcal{G}(K, F) \mid f|_A = \text{id}\}$$

$$f|_A = \text{id} \Leftrightarrow f|_A(\alpha_i) = \alpha_i \quad \forall i$$

$$k \in K = F(\alpha_1, \dots, \alpha_n) \xRightarrow{\substack{[2.21, \text{pg.18}]}} k = \frac{h(\alpha_1, \dots, \alpha_n)}{j(\alpha_1, \dots, \alpha_n)}, \quad h, j \in F[x_1, \dots, x_n]$$

$$f(k) \underset{f \text{ omomorfismo}}{=} \frac{fh(\alpha_1, \dots, \alpha_n)}{fj(\alpha_1, \dots, \alpha_n)} \underset{f|_F = \text{id}, f \text{ omo.}}{=} \frac{h(f(\alpha_1), \dots, f(\alpha_n))}{j(f(\alpha_1), \dots, f(\alpha_n))} \underset{f|_A = \text{id}}{=} \frac{h(\alpha_1, \dots, \alpha_n)}{j(\alpha_1, \dots, \alpha_n)} = k$$

$$f(k) = k \quad \forall k \in K \Rightarrow f = \text{id}_K$$

Quindi, $f|_A = \text{id} \Leftrightarrow f = \text{id}_K \Rightarrow \ker \Phi = [\text{id}] \Rightarrow \Phi$ e' iniettiva

□

Corollary 6.27. Sia $f(x) \in F[x]$ separabile, $K = CS(f(x), F)$, $\deg f(x) = n$. Si ha

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

Proof:

$$\begin{cases} f(x) \in F[x] \text{ separabile} \\ K = CS(f(x), F) \end{cases} \xRightarrow{\substack{[6.19, \text{pg.92}]}} F \subseteq K \text{ di Galois} \Rightarrow [K : F] = |\mathcal{G}(K, F)|$$

Per la prop. [6.26,pg.99], abbiamo la seguente immersione tra gruppi:

$$\Phi : \mathcal{G}(K, F) \hookrightarrow S_n$$

$$\text{Im } \Phi \leq S_n \xRightarrow{\substack{\text{Lagrange [AII,1.53,pg.19]}}} |\text{Im } \Phi| / |S_n| = n!$$

$$|\mathcal{G}(K, F)| \underset{\substack{\Phi \text{ iniettiva}}}{=} |\text{Im } \Phi| / n!$$

□

Definition 6.28. Sia H un gruppo di funzioni e A un insieme non vuoto.

$$H \text{ e' transitivo su } A \stackrel{\text{def}}{\Leftrightarrow} \forall \alpha_i, \alpha_j \in A \quad \exists \sigma \in H : \sigma(\alpha_i) = \alpha_j$$

Rievocando il concetto di orbita (vedi [AII,1.9,pg.72]) possiamo dire:

$$H \text{ e' transitivo su } A \Leftrightarrow \mathcal{O}_H(\alpha) = \{h(\alpha) \mid h \in H\} = A \quad \forall \alpha \in A$$

Proposition 6.29. Sia $f(x) \in F[x]$, $K = CS(f(x), F)$, $\deg f(x) = n \geq 1$, $G = \mathcal{G}(K, F)$, A l'insieme delle radici di $f(x)$. Si ha

$$G \text{ transitivo su } A \Leftrightarrow f(x) \text{ irriducibile in } F[x]$$

Nota: se $f(x)$ e' separabile, allora per la [6.26,pg.99], $G \simeq H \leq S_n$. Quindi per controllare che G sia transitivo, basta controllare che H sia transitivo su $\{1, \dots, n\}$. Cosi' facendo non dobbiamo considerare A (e quindi le radici di $f(x)$). Bisogna pero' determinare H .

Proof:

$$\langle 1 \rangle \text{ Dim } \Rightarrow$$

Sia $h(x) \in F[x]$ un fattore irriducibile di $f(x)$. Dimostriamo che $h(x) = f(x)$.

Sia $\alpha \in K$ una radice di $h(x)$

$$h(\alpha) = 0 \Rightarrow f(\alpha) = 0 \Rightarrow \alpha \in A \quad \underbrace{\Rightarrow}_{G \text{ transitivo su } A} \quad \mathcal{O}_G(\alpha) = A$$

$$\alpha_i \in A = \mathcal{O}_G(\alpha) \Rightarrow \exists \varphi \in G : \varphi(\alpha) = \alpha_i$$

$$\varphi \in G \subseteq \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.7, \text{pg.80}]} \quad h(\varphi(\alpha)) = \varphi(h(\alpha)) = \varphi(0) = 0 \Rightarrow \varphi(\alpha) = \alpha_i \text{ radice di } h(x)$$

$$\alpha_i \text{ radice di } h(x) \forall \alpha_i \in A \quad (1)$$

Quindi tutte le radici di $f(x)$ sono radici di $h(x)$, e quindi

$$(1) \Rightarrow f(x) \Big/ h(x)$$

$$h(x) \text{ fattore di } f(x) \Rightarrow h(x) \Big/ f(x)$$

$$\Rightarrow h(x) = f(x)$$

Perciò $f(x)$ è irriducibile in $F[x]$.

(2) Dim $\Leftarrow$

Dobbiamo dimostrare che

$$\forall \alpha_i, \alpha_j \in A \quad \exists \varphi \in G : \varphi(\alpha_i) = \alpha_j$$

Abbiamo:

$$\begin{cases} f(x) \text{ irrid. in } F[x] \\ \alpha_i, \alpha_j \text{ radici di } f(x) \end{cases} \quad \underbrace{\Rightarrow}_{[2.38, \text{pg.28}]} \quad \exists \psi : F(\alpha_i) \longrightarrow F(\alpha_j) \text{ isomorfismo t.c. } \begin{cases} \psi(\alpha_i) = \alpha_j \\ \psi|_F = \text{id} \end{cases} \quad (1)$$

Adesso cerchiamo di estendere ψ a una $\varphi \in G$ usando il thm [2.52, pg.38]:

$$\begin{cases} F \subseteq F(\alpha_i), F(\alpha_j) \subseteq K = F(\alpha_1, \dots, \alpha_n) \\ K = CS(f(x), F) \end{cases} \quad \underbrace{\Rightarrow}_{[2.54, \text{pg.42}]} \quad K = CS(f(x), F(\alpha_i)) = CS(f(x), F(\alpha_j)) \quad (2)$$

Sia $\psi' : F(\alpha_i)[x] \longrightarrow F(\alpha_j)[x]$ l'indotto di ψ , abbiamo

$$\psi'(f(x)) \quad \underbrace{=}_{\psi|_F = \text{id}, f(x) \in F[x]} \quad f(x)$$

$$K' = CS(\psi'(f(x)), F(\alpha_j)) = CS(f(x), F(\alpha_j)) \quad \underbrace{=}_{(2)} \quad K$$

Sia $F' = F(\alpha_i)$, $F'' = F(\alpha_j)$, e applichiamo il thm [2.52, pg.38]:

$$\begin{cases} \psi : F' \longrightarrow F'' \text{ isomorfismo} \\ f(x) = \psi'(f(x)) \\ F' \preceq K \quad \underbrace{=}_{(2)} \quad CS(f(x), F') \\ F'' \preceq K' = CS(\psi'(f(x)), F'') \end{cases} \quad \Rightarrow \quad \begin{cases} \exists \varphi : K \simeq K' = K \text{ isomorf.} \\ \varphi|_{F'} = \psi \end{cases}$$

Abbiamo così trovato la nostra φ , infatti,

$$\alpha_i \in F(\alpha_i) = F', \quad \varphi|_{F'} = \psi \Rightarrow \varphi(\alpha_i) = \psi(\alpha_i) \quad \underbrace{=}_{(1)} \quad \alpha_j$$

$$\begin{cases} \varphi : K \longrightarrow K \text{ isomorfismo} \\ \varphi|_F \quad \underbrace{=}_{F \subseteq F'} \quad \psi|_F \quad \underbrace{=}_{(1)} \quad \text{id} \end{cases} \quad \Rightarrow \quad \varphi \in \mathcal{G}(K, F) = G$$

□

Theorem 6.30. Sia $F \preceq K$ una estensione di Galois e sia $F \preceq L \preceq K$. Si ha

1. $[L : F] = \frac{|\mathcal{G}(K, F)|}{|\mathcal{G}(K, L)|} = \frac{[K : F]}{[K : L]}$
2. $F \preceq L$ e' di Galois $\Leftrightarrow \mathcal{G}(K, L) \leq \mathcal{G}(K, F)$ sottogruppo normale
3. $F \preceq L$ e' di Galois $\Rightarrow \mathcal{G}(L, F) \simeq \frac{\mathcal{G}(K, F)}{\mathcal{G}(K, L)}$ il gruppo quoziente

Ponendo $G = \mathcal{G}(K, F)$, $H = \mathcal{G}(K, L)$, $J = \mathcal{G}(L, F)$, diventano:

1. $[L : F] = \frac{|G|}{|H|} = \frac{[K : F]}{[K : L]}$
2. $F \preceq L$ e' di Galois $\Leftrightarrow H \leq G$ sottogruppo normale
3. $F \preceq L$ e' di Galois $\Rightarrow J \simeq \frac{G}{H}$ il gruppo quoziente

Proof:

(1) Dim 1.

$$F \preceq K \text{ Galois} \Rightarrow F \preceq K \text{ finita} \xRightarrow{\text{[2.18, pg.16]}} [K : L][L : F] = [K : F] \Leftrightarrow [L : F] = \frac{[K : F]}{[K : L]}$$

$$F \preceq K \text{ Galois} \xRightarrow{\text{[6.23, pg.96]}} L \preceq K \text{ Galois} \xRightarrow{\text{[6.19, pg.92]}} [K : L] = |\mathcal{G}(K, L)| = |H|$$

$$F \preceq K \text{ Galois} \xRightarrow{\text{[6.19, pg.92]}} [K : F] = |\mathcal{G}(K, F)| = |G|$$

$$[L : F] = \frac{[K : F]}{[K : L]} = \frac{|G|}{|H|}$$

(2) Dim 2.

(2.1) Dim $\Rightarrow$

Consideriamo la seguente mappa:

$$\phi : G \longrightarrow J$$

$$\varphi \in G \mapsto \varphi|_L$$

$$(2.1.1) \quad \phi \text{ e' ben posta: } \phi(\varphi) = \varphi|_L \in J = \mathcal{G}(L, F)$$

$$F \preceq K \text{ algebrica} \xRightarrow{\text{[2.45, pg.31]}} F \preceq L \text{ algebrica}$$

$$\text{Per Hp } F \preceq L \text{ e' di Galois} \xRightarrow{\text{[6.24, pg.96]}} \mathcal{I}(L, F) = \mathcal{G}(L, F) = J \quad (*)$$

$$F \preceq K \text{ di Galois} \Rightarrow F \preceq K \text{ algebrica} \xRightarrow{\text{[2.62, pg.49]}} \overline{F} = \overline{K}$$

$$\left\{ \begin{array}{l} \varphi|_L : L \longrightarrow K \subseteq \overline{K} = \overline{F} \\ (\varphi|_L)|_F \xRightarrow{F \subseteq L} \varphi|_F \xRightarrow{\varphi \in G = \mathcal{G}(K, F)} \text{id} \\ \varphi \in G \Rightarrow \varphi \text{ omomorf.} \Rightarrow \varphi|_L \text{ omomorf.} \\ F \preceq L \text{ algebrica} \end{array} \right. \Rightarrow \varphi|_L \in \mathcal{I}(L, F) \xRightarrow{(*)} J$$

⟨2.1.2⟩ ϕ e' un omomorfismo tra gruppi

Segue immediatamente dal fatto che ϕ e' ben posta:

$$\phi(fg) = (fg)|_L = fg|_L$$

$$\phi(f) \circ \phi(g) = f|_L g|_L$$

$$\phi(g) = g|_L \underbrace{\in}_{\text{passo 2.1.1}} J = \mathcal{G}(L, F) \Rightarrow g|_L : L \longrightarrow L \Rightarrow f|_L g|_L = fg|_L$$

$$\phi(f) \circ \phi(g) = f|_L g|_L = fg|_L = \phi(fg)$$

⟨2.1.3⟩ $\ker \phi = H$

$$\begin{cases} g \in G = \mathcal{G}(K, F) \\ \phi(g) = \text{id} \Leftrightarrow g|_L = \text{id} \end{cases} \underbrace{\Leftrightarrow}_{F \subseteq L} g \in \mathcal{G}(K, L) = H$$

Quindi $g \in \ker \phi \Leftrightarrow g \in H$

Poiche' $\ker \phi$ e' normale, anche H lo e'.

⟨2.1.4⟩ Dim 3.

Applicando il thm dell'omomorfismo tra gruppi (vedi [AII,1.147,pg.60]) all'omomorfismo ϕ , si ha

$$\frac{G}{\ker \phi} \simeq \text{Im } \phi \underbrace{\Leftrightarrow}_{H = \ker \phi} \frac{G}{H} \simeq \text{Im } \phi$$

Dimostriamo che $\text{Im } \phi = J$:

$$\text{Im } \phi \simeq \frac{G}{H} \Rightarrow |\text{Im } \phi| = \left| \frac{G}{H} \right| \underbrace{=}_{\text{[AII,1.114,pg.47]}} \frac{|G|}{|H|} \underbrace{=}_{\text{passo 1}} [L : F] \underbrace{=}_{F \preceq L \text{ Galois}} |\mathcal{G}(L, F)| = |J|$$

$$\begin{cases} \text{Im } \phi \subseteq J \\ |\text{Im } \phi| = |J| \\ J \text{ e' finito} \end{cases} \Rightarrow \text{Im } \phi = J$$

⟨2.2⟩ Dim $\Leftarrow$

Continuiamo la dimostrazione della 2., implicazione $\Leftarrow$.

Dobbiamo dimostrare che $F \preceq L$ e' di Galois. Lo faremo usando la caratterizzazione

$$[L : F] = |\mathcal{G}(L, F)| = |J|$$

Procediamo:

$$F \preceq K \text{ di Galois} \underbrace{\Rightarrow}_{\text{[6.23,pg.96]}} L \preceq K \text{ di Galois} \underbrace{\Rightarrow}_{\text{[6.19,pg.92]}} L = K^{\mathcal{G}(K, L)} = K^H \quad (3)$$

Riconsideriamo la mappa

$$\phi : G \longrightarrow J$$

$$\varphi \in G \mapsto \varphi|_L$$

Stavolta, per dimostrare che ϕ e' ben posta, sfrutteremo la normalita' di H .

⟨2.2.1⟩ ϕ e' ben posta: $\text{Im } \phi \subseteq J$

Preso $g \in G$ dimostriamo $\phi(g) = g|_L \in J = \mathcal{G}(L, F)$

$$g \in G \Rightarrow \begin{cases} g|_F = \text{id} \\ g|_L : L \longrightarrow K \\ g \text{ isomorfismo} \Rightarrow g|_L \text{ immersione} \end{cases} \quad (*)$$

$$g|_L \in \mathcal{G}(L, F) \Leftrightarrow \begin{cases} g|_L : L \longrightarrow L \text{ isomorfismo} \\ g|_F = \text{id} \end{cases} \underbrace{\Leftrightarrow}_{(*)} \text{Im } g|_L = L$$

Quindi, basta verificare che $\text{Im } g|_L = L$

(2.2.1.1) Dim. $\text{Im } g|_L \subseteq L$

Sia $\alpha \in L$.

$$g(\alpha) \in L \underbrace{=}_{(3)} K^H \Leftrightarrow h(g(\alpha)) = g(\alpha) \quad \forall h \in H$$

$$h(g(\alpha)) = g(\alpha) \underbrace{\Leftrightarrow}_{g \text{ isomorfismo}} g^{-1}hg(\alpha) = \alpha \quad (**)$$

$$h \in H \leq G \text{ normale} \underbrace{\Rightarrow}_{\text{caratterizz. sottogruppi normali [AII,1.104,pg.42]}} g^{-1}hg = h' \in H$$

$$(**) \Leftrightarrow h'(\alpha) = \alpha \quad \text{vero perche' } \alpha \in L = K^H$$

Quindi e' vero che $h(g(\alpha)) = g(\alpha) \quad \forall h \in H$

(2.2.1.2) $\text{Im } g|_L = L$

$$\text{Im } g|_L \subseteq L \Rightarrow g|_L : L \longrightarrow L$$

$$F \preceq K \text{ finita} \Rightarrow F \preceq L \text{ finita}$$

$$\left\{ \begin{array}{l} g|_L : L \longrightarrow L \\ (g|_L)|_F \underbrace{=}_{F \subseteq L} g|_F = \text{id} \\ L_F \text{ spazio vett. di dim. finita} \end{array} \right. \underbrace{\Rightarrow}_{[2.15, \text{pg.15}]} g|_L \text{ e' una applicazione lineare e quindi un endomorfismo}$$

$$g \text{ iniettiva} \Rightarrow g|_L \text{ iniettiva}$$

$$g|_L \text{ endomorfismo iniettivo} \underbrace{\Rightarrow}_{[\text{AL}, 8.1, \text{pg.50}]} g|_L \text{ e' un isomorfismo vettoriale} \Rightarrow \text{Im } g|_L = L$$

(2.2.2) ϕ e' un omomorfismo tra gruppi

Si procede come nel passo <3>2.

(2.2.3) $\ker \phi = H$

Si procede come nel passo <3>3.

In definitiva, per il thm dell'omomorfismo:

$$\frac{G}{H} \simeq \text{Im } \phi \leq J \quad (+)$$

$$\begin{aligned} F \subseteq L \text{ finita} & \underbrace{\Rightarrow}_{[6.10, \text{pg.84}]} [L : F] \geq |\mathcal{G}(L, F)| = |J| \underbrace{\geq}_{(+)} \left| \frac{G}{H} \right| \underbrace{=}_{[\text{AII}, 1.114, \text{pg.47}]} \frac{|G|}{|H|} \underbrace{=}_{\text{passo 1}} [L : F] \\ & \Rightarrow [L : F] = |\mathcal{G}(L, F)| \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} F \preceq L \text{ e' di Galois} \end{aligned}$$

□

Corollary 6.31. Sia $F \preceq K$ una estensione di Galois, e sia

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

$$H \leq G \text{ sottogruppo}$$

allora

1. $[K^H : F] = \frac{|G|}{|H|} = \frac{[K : F]}{[K : K^H]}$
2. $F \preceq K^H$ e' di Galois $\Leftrightarrow H \leq G$ sottogruppo normale
3. $F \preceq K^H$ e' di Galois $\Rightarrow \mathcal{G}(K^H, F) \simeq \frac{G}{H}$ il gruppo quoziente

Proof: Utilizzando la corrispondenza di Galois (vedi [6.25,pg.96]). abbiamo

$$H \leq G \Rightarrow F \preceq K^H \leq K$$

$$\mathcal{G}(K, K^H) = H \quad (1)$$

Ponendo $L = K^H$, e applicando il thm [6.30,pg.101]:

1. $[K^H : F] = \frac{|\mathcal{G}(K, F)|}{|\mathcal{G}(K, K^H)|} = \frac{[K : F]}{[K : K^H]}$
2. $F \preceq K^H$ e' di Galois $\Leftrightarrow \mathcal{G}(K, K^H) \leq \mathcal{G}(K, F)$ sottogruppo normale
3. $F \preceq K^H$ e' di Galois $\Rightarrow \mathcal{G}(K^H, F) \simeq \frac{\mathcal{G}(K, F)}{\mathcal{G}(K, K^H)}$

Per la (1), e considerando $G = \mathcal{G}(K, F)$:

1. $[K^H : F] = \frac{|G|}{|H|} = \frac{[K : F]}{[K : K^H]}$
2. $F \preceq K^H$ e' di Galois $\Leftrightarrow H \leq G$ sottogruppo normale
3. $F \preceq K^H$ e' di Galois $\Rightarrow \mathcal{G}(K^H, F) \simeq \frac{G}{H}$

che e' la tesi. □

Proposition 6.32. Sia $F \preceq K$ di Galois, $F \preceq L \preceq K$, $\varphi \in G = \mathcal{G}(K, F)$. Si ha

$$F \preceq \varphi(L) \preceq K$$

$\varphi(L)$ si chiama campo coniugato di L .

Proof:

$$F \subseteq L \subseteq K \Rightarrow \varphi(F) \subseteq \varphi(L) \subseteq \varphi(K)$$

$$\varphi \in \mathcal{G}(K, F) \Rightarrow \varphi|_F = \text{id} \Rightarrow \varphi(F) = F$$

$$\varphi \in \mathcal{G}(K, F) \Rightarrow \varphi : K \longrightarrow K \text{ surriettiva} \Rightarrow \varphi(K) = K$$

Resta da verificare che $\varphi(L)$ e' un sottocampo di K : siano $a, b \in L$, $b \neq 0$

$$L \text{ campo} \Rightarrow a - b, ab^{-1} \in L \quad \varphi(a) - \varphi(b) \underbrace{=}_{\varphi \text{ omomorf.}} \varphi(\underbrace{a - b}_{\in L}) \in \varphi(L)$$

$$\varphi(a)\varphi(b) = \varphi(\underbrace{ab}_{\in L}) \in \varphi(L)$$

□

Proposition 6.33. Sia $F \preceq K$ di Galois, $F \preceq L \preceq K$, $\varphi \in G = \mathcal{G}(K, F)$. Si ha

$$\mathcal{G}(K, \varphi(L)) = \varphi \mathcal{G}(K, L) \varphi^{-1}$$

$$\text{dove } \varphi \mathcal{G}(K, L) \varphi^{-1} \stackrel{\text{def}}{=} \{ \varphi g \varphi^{-1} \mid g \in \mathcal{G}(K, L) \}$$

Proof:

(1) Dim $\supseteq$

Sia $g \in \mathcal{G}(K, L)$. Dimostriamo che $\varphi g \varphi^{-1} \in \mathcal{G}(K, \varphi(L))$.

$\varphi g \varphi^{-1}$ e' composizione di automorfismi su $K \Rightarrow \varphi g \varphi^{-1}$ e' un automorfismo su K

Resta da verificare che $(\varphi g \varphi^{-1})|_{\varphi(L)} = \text{id}$. Sia $b \in \varphi(L)$

$$b \in \varphi(L) \Rightarrow \exists a \in L : \varphi(a) = b$$

$$(\varphi g \varphi^{-1})(b) = \varphi g \varphi^{-1} \varphi(a) = \varphi g(a) \underbrace{\quad}_{g|_L = \text{id}, a \in L} \varphi(a) = b$$

Quindi

$$\begin{cases} \varphi g \varphi^{-1} : K \longrightarrow K \text{ isomorfismo} \\ (\varphi g \varphi^{-1})|_{\varphi(L)} = \text{id} \end{cases} \Rightarrow \varphi g \varphi^{-1} \in \mathcal{G}(K, \varphi(L))$$

(2) Dim $\subseteq$

Sia $\psi = \varphi^{-1}, L' = \varphi(L)$.

$$\varphi \in G = \mathcal{G}(K, F) \underbrace{\Rightarrow}_{G \text{ gruppo}} \psi = \varphi^{-1} \in G$$

$$F \preceq L \preceq K \underbrace{\Rightarrow}_{[6.32, \text{pg. } 105]} F \preceq L' \preceq K$$

Allora, per quanto dimostrato nel passo precedente, abbiamo

$$\psi \mathcal{G}(K, L') \psi^{-1} \subseteq \mathcal{G}(K, \psi(L')) \Leftrightarrow \varphi^{-1} \mathcal{G}(K, \varphi(L)) \varphi \subseteq \mathcal{G}(K, L) \underbrace{\Leftrightarrow}_{(*)} \mathcal{G}(K, \varphi(L)) \subseteq \varphi \mathcal{G}(K, L) \varphi^{-1}$$

(*) Infatti,

$$\varphi^{-1} g \varphi \in \varphi^{-1} \mathcal{G}(K, \varphi(L)) \varphi \subseteq \mathcal{G}(K, L) \Rightarrow \exists g' \in \mathcal{G}(K, L) : \varphi^{-1} g \varphi = g' \Leftrightarrow g = \varphi g' \varphi^{-1} \in \varphi \mathcal{G}(K, L) \varphi^{-1}$$

□

Proposition 6.34. Sia

1. $F \preceq K, F \preceq L \preceq K$
2. $L = F(\alpha_1, \dots, \alpha_n), \alpha_1, \dots, \alpha_n \in K$
3. $\varphi \in \mathcal{I}(K, F)$, con $\varphi(\alpha_i) = \beta_i \quad \forall i = 1, \dots, n$

Si ha

$$\varphi(L) = \varphi(F(\alpha_1, \dots, \alpha_n)) = F(\beta_1, \dots, \beta_n)$$

Proof:

$$\varphi \in \mathcal{I}(K, F) \Rightarrow \varphi|_F = \text{id}$$

$$\varphi \in \mathcal{I}(K, F) \xRightarrow{\substack{\text{[6.3,pg.78]} \\ \varphi \text{ e' iniettiva}}} \varphi \text{ e' omomorfismo tra anelli} \xRightarrow{\text{Im } \varphi|_L = \varphi(L) \simeq L}$$

$$\begin{cases} L \text{ campo} \\ \varphi(L) \simeq L \end{cases} \Rightarrow \varphi(L) = \varphi(F(\alpha_1, \dots, \alpha_n)) \text{ campo}$$

$$F(\alpha_1, \dots, \alpha_n) \xRightarrow{\substack{\text{[2.21,pg.18]} \\ \varphi \text{ omomorfismo}}} \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in F[x_1, \dots, x_n], g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

$$\begin{aligned} \varphi \left(\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \right) &\xRightarrow{\varphi \text{ omomorfismo}} \frac{\varphi f(\alpha_1, \dots, \alpha_n)}{\varphi g(\alpha_1, \dots, \alpha_n)} \xRightarrow{\varphi|_F = \text{id}, \varphi \text{ omo.}} \frac{f(\varphi(\alpha_1), \dots, \varphi(\alpha_n))}{g(\varphi(\alpha_1), \dots, \varphi(\alpha_n))} = \\ &= \frac{f(\beta_1, \dots, \beta_n)}{g(\beta_1, \dots, \beta_n)} \in F(\beta_1, \dots, \beta_n) \end{aligned}$$

Quindi, $\varphi(F(\alpha_1, \dots, \alpha_n)) \subseteq F(\beta_1, \dots, \beta_n)$

$$\begin{cases} \beta_1, \dots, \beta_n \xRightarrow{\beta_i = \varphi(\alpha_i)} \varphi(F(\alpha_1, \dots, \alpha_n)) \\ F \xRightarrow{\varphi|_F = \text{id}} \varphi(F(\alpha_1, \dots, \alpha_n)) \\ \varphi(F(\alpha_1, \dots, \alpha_n)) \text{ campo} \end{cases} \Rightarrow F(\beta_1, \dots, \beta_n) \subseteq \varphi(F(\alpha_1, \dots, \alpha_n))$$

Quindi $F(\beta_1, \dots, \beta_n) = \varphi(F(\alpha_1, \dots, \alpha_n))$

□

6.1 Teorema fondamentale dell'algebra

Proposition 6.35.

$$\mathbb{C} \text{ e' chiuso} \Leftrightarrow (f(x) \in \mathbb{R}[x], \deg f(x) \geq 1 \Rightarrow \exists \alpha \in \mathbb{C} : f(\alpha) = 0)$$

Proof:

(1) Dim. $\Rightarrow$

$$f(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$$

Ma $\mathbb{C}$ e' chiuso, e quindi per definizione, $f(x)$ ha una radice in $\mathbb{C}$.

(1) Dim. $\Leftarrow$

Consideriamo l'operazione di coniugazione:

$$\bar{\cdot} : \mathbb{C} \longrightarrow \mathbb{C}$$

$$z \mapsto \bar{z}$$

$\bar{\cdot}$ e' un omomorfismo di campi, infatti,

$$\overline{a+b} = \bar{a} + \bar{b}$$

$$\overline{ab} = \bar{a}\bar{b}$$

e' inoltre un isomorfismo (la sua inversa e' se stesso).

Quindi per la prop [1.13,pg.3], anche il suo indotto

$$\hat{\bar{\cdot}} : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$$

e' un isomorfismo.

Per dimostrare che $\mathbb{C}$ e' chiuso, consideriamo un generico $h(x) \in \mathbb{C}[x]$, con $\deg h(x) \geq 1$, e

vediamo che $h(x)$ ha una radice $\alpha \in \mathbb{C}$.

Sia $f(x) = h(x)\widehat{h}(x)$

$$\widehat{f}(x) = \widehat{h(x)\widehat{h}(x)} \quad \underbrace{\quad}_{\widehat{\text{omomorfismo}}} \quad \widehat{h}(x)\widehat{\widehat{h}(x)} = \widehat{h}(x)h(x) = f(x)$$

$$\widehat{f}(x) = f(x) \Rightarrow f(x) \in \mathbb{R}[x] \xRightarrow[\text{Hp}]{\quad} \exists \alpha \in \mathbb{C} : f(\alpha) = 0 \Leftrightarrow h(\alpha)\widehat{h}(\alpha) = 0 \Leftrightarrow h(\alpha) = 0 \vee \widehat{h}(\alpha) = 0 \quad (1)$$

Se $h(\alpha) = 0$, α e' una radice di $h(x)$. Supponiamo allora che $h(\alpha) \neq 0$. Per la (1)

$$\widehat{h}(\alpha) = 0 \Rightarrow \widehat{\widehat{h}(\alpha)} = \overline{0} \Leftrightarrow h(\overline{\alpha}) = 0 \Rightarrow \overline{\alpha} \text{ e' radice di } h(x)$$

□

Proposition 6.36. Sia $f(x) \in \mathbb{R}[x]$, allora

$$\deg f(x) \text{ dispari} \Rightarrow \exists \alpha \in \mathbb{R} : f(\alpha) = 0$$

Proposition 6.37.

$$f(x) = a_0 + \dots + a_d x^d, \quad d \text{ dispari}$$

Supponiamo $a_d > 0$ (analogamente si vede per $a_d < 0$). Si ha

$$\lim_{x \rightarrow \infty} f(x) = \lim_{x \rightarrow \infty} a_d x^d \underbrace{\quad}_{a_d > 0} = +\infty$$

Quindi, definitivamente $f(x)$ sara' positivo. Allora esiste $b \in \mathbb{R} : f(b) > 0$.

$$\lim_{x \rightarrow -\infty} f(x) = \lim_{x \rightarrow -\infty} a_d x^d \underbrace{\quad}_{a_d > 0, \quad d \text{ dispari}} = -\infty$$

Quindi, definitivamente $f(x)$ sara' negativo. Allora esiste $a \in \mathbb{R} : f(a) < 0$.

$$\begin{cases} f(a)f(b) < 0 \\ f \text{ continua} \end{cases} \quad \underbrace{\quad}_{\text{thm dell'esistenza dello zero}} \quad \Rightarrow \quad \exists \alpha \in]\min\{a, b\}, \max\{a, b\}[: f(\alpha) = 0$$

Proposition 6.38. Sia $f(x) \in \mathbb{C}[x]$

$$\deg f(x) = 2 \Rightarrow f(x) \text{ si spezza linearmente in } \mathbb{C}[x]$$

Proof:

$$f(x) = ax^2 + bx + c$$

Le sue due radici sono

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (1)$$

dove

$$b^2 - 4ac = \rho(\cos \theta + i \sin \theta)$$

$$\sqrt{b^2 - 4ac} = \sqrt{\rho} \left(\cos \frac{\theta}{2} + i \sin \frac{\theta}{2} \right)$$

$\sqrt{\rho} \in \mathbb{R}$, infatti, per il thm dei valori intermedi, x^2 ammette tutti i valori tra il suo $\inf = 0$ e $\sup = +\infty$, quindi

$$\exists \gamma \in [0, +\infty[: \gamma^2 = \rho \Leftrightarrow \gamma = \sqrt{\rho} \in \mathbb{R}$$

Quindi tutti gli elementi fin'ora esposti stanno in $\mathbb{C}$, e in particolare le radici di $f(x)$ sono in $\mathbb{C}$. Quindi per Ruffini, $f(x)$ si spezza linearmente in $\mathbb{C}$. □

Theorem 6.39.

$\mathbb{C}$ e' algebricamente chiuso

Proof: Grazie alla prop [6.35,pg.107], basta dimostrare che preso $\Phi(x) \in \mathbb{R}[x]$, $\deg \Phi(x) \geq 1$ esiste $\alpha \in \mathbb{C} : \Phi(\alpha) = 0$.

Se $\Phi(x)$ e' irriducibile in $\mathbb{C}[x]$, sia $f(x) = \Phi(x)$, altrimenti sia $f(x)$ un suo fattore irriducibile e monico in $\mathbb{C}[x]$. Dimostreremo che $f(x)$ ha un radice in $\mathbb{C}$.

Sia $L = CS(f(x), \mathbb{C}) = \mathbb{C}(\alpha_1, \dots, \alpha_n)$, dove $\alpha_1, \dots, \alpha_n \in L$ sono le radici di $f(x)$.

(1) $\mathbb{C} \preceq L$ e' di Galois

$$\begin{aligned} & \left\{ \begin{array}{l} \mathbb{C} \preceq L \text{ algebrica} \\ \text{ch} L = 0 \end{array} \right. \xRightarrow{[3.23, \text{pg.60}]} L \preceq \mathbb{C} \text{ e' separabile } (*) \\ & \left\{ \begin{array}{l} f(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x] \text{ irriducibile} \\ f(\alpha_1) = 0 \\ f(x) \text{ monico} \end{array} \right. \xRightarrow{[2.30, \text{pg.24}]} f(x) = P_{\min}(\alpha_1, \mathbb{C}) \text{ che e' separabile per la } (*) \\ & \left\{ \begin{array}{l} f(x) \in \mathbb{C}[x] \text{ separabile} \\ L = CS(f(x), \mathbb{C}) \end{array} \right. \xRightarrow{[6.19, \text{pg.92}]} \mathbb{C} \preceq L \text{ e' di Galois} \end{aligned}$$

(2) $\mathbb{R} \preceq L$ e' di Galois

Se $f(i) = 0 \vee f(-i) = 0$ sia $g(x) = f(x)$, altrimenti sia $g(x) = f(x)(x^2 + 1)$. Poiche' $x^2 + 1$ e' separabile (le sue radici sono ± 1) e anche $f(x)$ e' separabile, $g(x)$ e' ancora separabile.

$$\begin{aligned} & \left\{ \begin{array}{l} [\mathbb{R}(i) : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2 \\ \mathbb{R}(i) \subseteq \mathbb{C} \end{array} \right. \Rightarrow \mathbb{R}(i) = \mathbb{C} \\ & CS(g(x), \mathbb{R}) = \mathbb{R}(\alpha_1, \dots, \alpha_n, i) = \mathbb{R}(i)(\alpha_1, \dots, \alpha_n) \xRightarrow{\mathbb{R}(i)=\mathbb{C}} \mathbb{C}(\alpha_1, \dots, \alpha_n) = L \\ & \left\{ \begin{array}{l} L = CS(g(x), \mathbb{R}) \\ g(x) \text{ separabile} \end{array} \right. \xRightarrow{[6.19, \text{pg.92}]} \mathbb{R} \subseteq L \text{ e' di Galois} \end{aligned}$$

Consideriamo la catena

$$\mathbb{R} \preceq \mathbb{C} \preceq L$$

abbiamo

$$[\mathbb{C} : \mathbb{R}] = 2 \xRightarrow{[2.18, \text{pg.16}]} 2 \nmid [L : \mathbb{R}] \Leftrightarrow [L : \mathbb{R}] = 2m = 2^{t+1}q, \text{ con } q \text{ dispari}$$

In pratica, abbiamo scritto $2m$ mettendo in evidenza tutti i fattori 2, ovvero

$$t + 1 = \max \left\{ z \in \mathbb{N} \mid 2^z \nmid [L : \mathbb{R}] \right\}$$

(3) Dim. che $q = 1$

$$\begin{aligned} & \mathbb{R} \preceq L \text{ di Galois } (*) \\ & |\mathcal{G}(L, \mathbb{R})| \xRightarrow{(*), [6.19, \text{pg.92}]} [L : \mathbb{R}] = 2^{t+1}q \xRightarrow{[AII, 2.8, \text{pg.83}]} \exists H \leq \mathcal{G}(L, \mathbb{R}) : |H| = 2^{t+1} \end{aligned}$$

Per la corrispondenza di Galois (vedi [6.25,pg.96]) abbiamo:

$$\begin{aligned} & \mathbb{R} \preceq L^H \preceq L \\ & \mathcal{G}(L, L^H) = H \quad (**) \end{aligned}$$

inoltre

$$\begin{aligned}
& \mathbb{R} \preceq L \text{ di Galois} \quad \underbrace{\Rightarrow}_{[6.23, \text{pg.} 96]} \quad L^H \preceq L \text{ di Galois} \quad \underbrace{\Rightarrow}_{[6.19, \text{pg.} 92]} \quad [L : L^H] = |\mathcal{G}(L, L^H)| \underbrace{=}_{(**)} |H| = 2^{t+1} \\
& \begin{cases} [L : \mathbb{R}] = 2^{t+1}q \\ [L : L^H] = 2^{t+1} \end{cases} \quad \underbrace{\Rightarrow}_{[2.18, \text{pg.} 16]} \quad [L^H : \mathbb{R}] = q \\
& \mathbb{R} \preceq L \text{ Galois} \Rightarrow \mathbb{R} \preceq L \text{ separabile} \quad \underbrace{\Rightarrow}_{[3.32, \text{pg.} 68]} \quad \mathbb{R} \preceq L^H \text{ separabile} \\
& \mathbb{R} \preceq L^H \text{ finita} \quad \underbrace{\Rightarrow}_{[2.44, \text{pg.} 31]} \quad \mathbb{R} \preceq L^H \text{ fin. gen.} \\
& \begin{cases} \mathbb{R} \preceq L^H \text{ separabile} \\ \mathbb{R} \preceq L^H \text{ fin. gen.} \end{cases} \quad \underbrace{\Rightarrow}_{[3.29, \text{pg.} 65]} \quad L^H = \mathbb{R}(\beta) \\
& \mathbb{R} \preceq L^H \text{ finita} \Rightarrow \mathbb{R} \preceq L^H \text{ algebrica} \Rightarrow \beta \text{ algebrico su } \mathbb{R} \Rightarrow \exists p(x) = P_{\min}(\beta, \mathbb{R}) \\
& \deg p(x) = [L^H : \mathbb{R}] = q \\
& \begin{cases} \deg p(x) = q \text{ dispari} \\ p(x) \in \mathbb{R}[x] \end{cases} \quad \underbrace{\Rightarrow}_{[6.36, \text{pg.} 108]} \quad \exists r \in \mathbb{R} : p(r) = 0 \\
& \begin{cases} p(x) \text{ irriducibile} \\ p(r) = 0 \end{cases} \quad \underbrace{\Rightarrow}_{\text{Ruffini}} \quad \deg p(x) = 1 \\
& q = [L^H : \mathbb{R}] = \deg p(x) = 1 \\
(4) \quad t = 0
\end{aligned}$$

$$\begin{aligned}
& \mathbb{R} \preceq \mathbb{C} \preceq L \\
& [L : \mathbb{R}] = 2^{t+1}q \underbrace{=}_{q=1} 2^{t+1} \\
& \begin{cases} [L : \mathbb{R}] = 2^{t+1} \\ [\mathbb{C} : \mathbb{R}] = 2 \end{cases} \Rightarrow [L : \mathbb{C}] = 2^t
\end{aligned}$$

Supponiamo per assurdo che $t \geq 1$.

$$\begin{aligned}
& \mathbb{C} \preceq L \text{ e' di Galois (passo 1)} \Rightarrow |\mathcal{G}(L, \mathbb{C})| = [L : \mathbb{C}] = 2^t \Rightarrow \mathcal{G}(L, \mathbb{C}) \text{ e' un } 2 - \text{gruppo} \\
& \underbrace{\Rightarrow}_{[\text{AII}, 2.5, \text{pg.} 80]} \quad \exists N \leq \mathcal{G}(L, \mathbb{C}) \text{ normale : } |N| = 2^{t-1} \quad (2)
\end{aligned}$$

Utilizzando la corrispondenza di Galois (vedi [6.25, pg. 96]). abbiamo

$$\begin{aligned}
& \mathbb{C} \preceq L^N \preceq L \\
& \mathcal{G}(L, L^N) = N
\end{aligned}$$

allora

$$\left\{ \begin{array}{l} \mathbb{C} \preceq L \text{ di Galois} \\ \mathcal{G}(L, L^N) = N \leq \mathcal{G}(L, \mathbb{C}) \text{ normale} \end{array} \right. \xRightarrow{\substack{[6.30, \text{pg.101}]}} \mathbb{C} \preceq L^N \text{ e' di Galois} \xRightarrow{\substack{[6.19, \text{pg.92}]}} \mathbb{C} \preceq L^N \text{ separabile}$$

$\mathbb{C} \preceq L \text{ finita} \Rightarrow \mathbb{C} \preceq L^N \text{ finita} \Rightarrow \mathbb{C} \preceq L^N \text{ fin. gen.}$

$$\left\{ \begin{array}{l} \mathbb{C} \preceq L^N \text{ fin. gen.} \\ \mathbb{C} \preceq L^N \text{ separabile} \end{array} \right. \xRightarrow{\substack{[3.29, \text{pg.65}]}} \exists \gamma : L^N = \mathbb{C}(\gamma)$$

$\mathbb{C} \preceq L^N \text{ finita} \Rightarrow \mathbb{C} \preceq L^N \text{ algebrica} \Rightarrow \gamma \text{ algebrico su } \mathbb{C} \Rightarrow \exists q(x) = P_{\min}(\gamma, \mathbb{C})$

$\mathbb{C} \preceq L \text{ di Galois} \xRightarrow{\substack{[6.23, \text{pg.96}]}} L^N \preceq L \text{ di Galois}$

$$[L : L^N] \xRightarrow{\substack{L^N \preceq L \text{ di Galois, [6.19, pg.92]}}} |\mathcal{G}(L, L^N)| = |N| \xRightarrow{(2)} 2^{t-1}$$

$$\left\{ \begin{array}{l} [L : \mathbb{C}] = 2^t \\ [L : L^N] = 2^{t-1} \end{array} \right. \xRightarrow{\substack{[2.18, \text{pg.16}]}} [L^N : \mathbb{C}] = \frac{2^t}{2^{t-1}} = 2$$

$\deg q(x) = \deg P_{\min}(\gamma, \mathbb{C}) = [\mathbb{C}(\gamma) : \mathbb{C}] = [L^N : \mathbb{C}] = 2$

$$\left\{ \begin{array}{l} \deg q(x) = 2 \\ q(x) \in \mathbb{C}[x] \end{array} \right. \xRightarrow{\substack{[6.38, \text{pg.108}]}} q(x) \text{ e' riducibile in } \mathbb{C}[x]$$

assurdo contro $q(x) = P_{\min}(\gamma, \mathbb{C})$.

(5) Q.E.D.

$$[L : \mathbb{C}] = 2^t \xRightarrow{\substack{\text{passo 4}}} 2^0 = 1$$

$$\left\{ \begin{array}{l} \mathbb{C} \subseteq L \\ [L : \mathbb{C}] = 1 \end{array} \right. \Rightarrow \mathbb{C} = L = \mathbb{C}(\alpha_1, \dots, \alpha_n) \Rightarrow \alpha_1, \dots, \alpha_n \in \mathbb{C}$$

quindi $f(x)$ ha tutte le radici in $\mathbb{C}$. Noi volevamo dimostrare che ne aveva almeno una. $\square$

6.2 Estensioni ciclotomiche

Lemma 6.40. *Sia $n \geq 1$, $(n, p) = 1$, p primo, $q = p^r$, allora*

$$n/q^m - 1 \Leftrightarrow o(q)/m$$

dove $o(q)$ e' l'ordine di q in $U(\mathbb{Z}_n)$, gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_n$. Quindi,

$$\min \left\{ m \mid n/q^m - 1 \right\} = o(q)$$

Proof:

$$(n, p) = 1 \xLeftrightarrow[q=p^r] (n, q) = 1 \xLeftrightarrow[\text{Vedi AI}] q \in U(\mathbb{Z}_n)$$

$$n/q^m - 1 \Leftrightarrow q^m = 1 \text{ in } U(\mathbb{Z}_n) \Leftrightarrow o(q) \mid m$$

$\square$

Proposition 6.41. Osservazione generale su U_n e $x^n - a$.

Sia $f(x) = x^n - a \in F[x]$, F campo, $a \neq 0$. Le radici di $f(x)$ sono:

$$b, \omega_1 b, \omega_2 b, \dots, \omega_m b \in CS(f(x), F)$$

$$\text{dove } b^n = a, \quad U_n = \{1, \omega_1, \dots, \omega_m\}$$

$(U_n, \cdot)$ e' l'insieme delle radici n -esime dell'unita' nel campo F , ovvero

$$U_n = \{\xi \in CS(x^n - 1, F) \mid \xi^n - 1 = 0\}$$

$(U_n, \cdot)$ e' un gruppo moltiplicativo.

Si distinguono i seguenti casi:

CASE: $\text{ch}F = 0$

Qui, ritroviamo l' U_n classico, ovvero

$$U_n = \{\xi \in \mathbb{C} \mid \xi^n - 1 = 0\}$$

e le radici di $f(x)$ sono tutte distinte, ovvero $f(x)$ e' separabile.

Inoltre, U_n e' ciclico (vedi [AII, 1.16, pg.4]) $U_n = \langle \omega \rangle$, con $|U_n| = n$, quindi le radici di $f(x)$ sono

$$b, \omega b, \omega^2 b, \dots, \omega^{n-1} b \in CS(f(x), F)$$

CASE: $\text{ch}F = p$, $p \nmid n$

Allora

$$U_n = \{1\}$$

e le radici di $f(x)$ si riducono all'unica radice b (quindi $f(x)$ non e' separabile).

CASE: $\text{ch}F = p$, $p \nmid n$, F finito

1. U_n e' ciclico

2. $U_n \subseteq F \Leftrightarrow n \mid |F| - 1$

3. Se $|F| = q$, ovvero $F \simeq F_q$, allora

la piu' piccola estensione $F \subseteq K$ t.c. $U_n \subseteq K$ e' data da un campo K t.c. $|K| = q^m$, ovvero $K \simeq F_{q^m}$

dove $m = o(q) = \text{ordine di } q \text{ in } U(\mathbb{Z}_n)$

CASE: $\text{ch}F = p$, $p \nmid n$, F infinito

Cosa si puo' dire?

Proof: Sia $K = CS(x^n - 1, F)$.

(1) $(U_n, \cdot)$ e' un gruppo

$$1 \not\equiv 0 \Rightarrow 0 \text{ non e' radice di } x^n - 1 \Rightarrow 0 \notin U_n$$

[1.1, pg.1]

$$\begin{cases} U_n \subseteq K \\ 0 \notin U_n \end{cases} \Rightarrow U_n \subseteq K^*$$

Allora, basta verificare che $(U_n, \cdot) \leq (K^*, \cdot)$, ovvero che

$$ab^{-1} \in U_n \quad \forall a, b \in U_n$$

Quindi,

$$a, b \in U_n \Rightarrow a^n = b^n = 1$$

$$(ab^{-1})^n \underbrace{=}_{a, b \in U_n \subseteq K^* \text{ campo}} a^n (b^n)^{-1} = 1 \Rightarrow (ab^{-1})^n - 1 = 0 \Rightarrow ab^{-1} \in U_n$$

Siano $(\omega_0 = 1), \omega_1, \dots, \omega_m$ gli elementi distinti di U_n (U_n e' necessariamente finito perche' $x^n - 1$ ammette un numero finito di radici).

Poiche'

$$(b\omega_i)^n = b^n \omega_i^n = a \Rightarrow b\omega_i \text{ radice di } x^n - a$$

$$\xi \text{ radice di } x^n - a \Leftrightarrow \xi^n = a = b^n \underbrace{\Leftrightarrow}_{a \neq 0 \Leftrightarrow b \neq 0} \frac{\xi^n}{b^n} = 1 \Leftrightarrow \left(\frac{\xi}{b}\right)^n = 1 \Leftrightarrow \frac{\xi}{b} \in U_n \Leftrightarrow \frac{\xi}{b} = \omega_i \Leftrightarrow \xi = \omega_i b$$

si ha che

$$\{\text{radici di } f(x) = x^n - a\} = \{b\omega_i \mid i = 0, \dots, m\}$$

Esaminiamo adesso i vari casi.

CASE: $\text{ch}F = 0$

U_n e' ciclico: $U_n = \langle \omega \rangle$, con $|U_n| = n$ (vedi [AII, 1.16, pg.4]). Quindi, le radici di $f(x) = x^n - b^n \in F[x]$ sono

$$b, \omega b, \omega^2 b, \dots, \omega^{n-1} b$$

$f(x)$ e' separabile, infatti,

$$f'(x) = nx^{n-1} = 0 \Leftrightarrow n = 0 \vee x = 0 \Leftrightarrow \begin{cases} \text{ch}F \neq 0 \\ \text{ch}F/n \end{cases} \vee x = 0 \underbrace{\Leftrightarrow}_{\text{ch}F=0} x = 0 \quad (*)$$

$$\xi \text{ e' radice multipla di } f(x) \underbrace{\Leftrightarrow}_{[1.17, \text{pg.6}]} f'(\xi) = 0 \underbrace{\Leftrightarrow}_{(*)} \xi = 0$$

$$\Rightarrow \underbrace{\exists i : \omega^i b = 0}_{\text{le radici di } f(x) \text{ sono } \omega^i b} \underbrace{\Leftrightarrow}_{b \neq 0} \omega^i = 0 \underbrace{\Leftrightarrow}_{K \text{ e' un dominio}} \omega = 0$$

assurdo contro $0 \notin U_n$.

Quindi $f(x)$ non ha radici multiple, ovvero e' separabile.

CASE: $\text{ch}F = p, \quad p \nmid n$

$$x^n - 1 = x^n - 1^n \underbrace{=}_{[1.20, \text{pg.7}]} (x - 1)^n \Rightarrow U_n = \{1\}$$

e quindi

$$b = \omega_1 b = \omega_2 b = \dots \omega_m b$$

CASE: $\text{ch}F = p, \quad p \nmid n, \quad F$ finito

(1.1) $(U_n, \cdot)$ e' ciclico

$$\begin{cases} F^* \text{ e' ciclico (vedi [3.8, pg.53])} \\ U_n \leq F^* \end{cases} \underbrace{\Rightarrow}_{[AII, 1.39, \text{pg.13}]} U_n \text{ ciclico (1)}$$

(1.2) Dim. 2.

(1.2.1) Dim. $\Rightarrow$

$$U_n \leq F^*, \quad U_n, F^* \text{ gruppi} \underbrace{\Rightarrow}_{\text{Lagrange [AII, 1.53, pg.19]}} n = |U_n| \mid |F^*| = |F| - 1$$

(1.2.2) Dim. $\Leftarrow$

$$n \nmid |F^*|, \quad F^* \text{ ciclico} \quad \underbrace{\Rightarrow}_{[\text{AII}, 1.42, \text{pg.} 14]} \quad \exists! H \leq F^* : |H| = n \quad (2)$$

$$|H| = n \quad \underbrace{\Rightarrow}_{\text{Lagrange } [\text{AII}, 1.53, \text{pg.} 19]} \quad h^n = 1 \quad \forall h \in H \Rightarrow H \subseteq U_n$$

$$\begin{cases} H \subseteq U_n \\ |H| = n = |U_n| \end{cases} \Rightarrow U_n = H \leq F^*$$

(1.3) Dim 3.

Per la prop [3.17, pg. 57] possiamo scrivere

$$F = F_q \subseteq K = F_{q^m}$$

Per la 2.

$$U_n \subseteq K \Leftrightarrow n \nmid |K| - 1 = q^m - 1 \quad \underbrace{\Leftrightarrow}_{p \nmid n \Leftrightarrow (n,p)=1, \text{ lemma } [6.40, \text{pg.} 111]} \quad m = o(q) \text{ in } U(\mathbb{Z}_n)$$

□

Theorem 6.42. Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unit . Poniamo

$$f(x) = x^n - 1$$

$$f_m(x) = \prod_{u \in U_n : U_m = \langle u \rangle} x - u \quad \text{dove } m \nmid n$$

φ funzione di Eulero, ovvero $\varphi(n) = |\{m \in \mathbb{N} \mid (m, n) = 1, m < n\}|$
dove $(m, n) = \text{MCD}(m, n)$

si ha

1. $f(x) = \prod_{m \nmid n} f_m(x)$
2. $f_n(x) \in \mathbb{Z}[x], \quad f_n(x) = P_{\min}(\omega, \mathbb{Q})$
3. $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg f_n(x) = \varphi(n)$
4. $\mathbb{Q} \preceq \mathbb{Q}(\omega)$ e' di Galois

Proof:

(1) Dim 1.

Per la prop [1.19, pg. 7] le radici di $f(x)$ sono

$$(1 = \omega^n), \omega, \omega^2, \dots, \omega^{n-1}$$

Quindi

$$f(x) = \prod_{i=0}^{n-1} x - \omega^i$$

Sia $m \leq n$. Osserviamo che preso un elemento $u \in U_n$,

$$U_m = \langle u \rangle \Leftrightarrow o(u) = m \quad (*)$$

$$f_m(x) = \prod_{u \in U_n : U_m = \langle u \rangle} x - u \quad \underbrace{=}_{(*)} \prod_{u \in U_n : o(u)=m} x - u$$

$$(1.1) \quad U_n = \left\{ u \in U_n \mid o(u) = m, \quad m \nmid n \right\}$$

Basta dimostrare $\subseteq$.

$$u \in U_n \xRightarrow{\text{[AII,1.54,pg.19]}} o(u)/|U_n| = n \Rightarrow u \in \left\{ u \in U_n \mid o(u) = m, \ m \nmid n \right\}$$

Allora,

$$f(x) = \prod_{i=0}^{n-1} x - \omega^i \xRightarrow{U_n = \langle \omega \rangle} \prod_{u \in U_n} x - u \xRightarrow{\text{passo 1.1}} \prod_{u \in U_n: o(u)=m, \ m \nmid n} x - u = \prod_{m \nmid n} f_m(x)$$

(2) $\deg f_n(x) = \varphi(n)$

Abbiamo visto che

$$f_n(x) = \prod_{u \in U_n: U_n = \langle u \rangle} x - u$$

Allora, basta contare gli elementi di $\{u \in U_n : U_n = \langle u \rangle\}$.

$$u \in U_n = \langle \omega \rangle \Leftrightarrow \exists i : \omega^i = u, \ i < n$$

$$U_n = \langle u \rangle = \langle \omega^i \rangle \xRightarrow{\text{[AII,1.45,pg.16]}} (i, n) = 1 \quad (*)$$

$$|\{u \in U_n \mid U_n = \langle u \rangle\}| \xRightarrow{(*)} |\{\omega^i \in U_n \mid (i, n) = 1, \ i < n\}| = |\{i \mid (i, n) = 1, \ i < n\}| = \varphi(n)$$

(3) Dim 2.

PROOF SKETCH: $f_n(x)$ e' monico, $f_n(\omega) = 0$. Per vedere che $f_n(x) = P_{\min}(\omega, \mathbb{Q})$, basta allora dimostrare che $f_n(x)$ e' irriducibile in $\mathbb{Q}[x]$. Utilizzeremo la prop [AI,23.1,pg.112] per poter dimostrare che $f_n(x)$ e' irriducibile in $\mathbb{Z}[x]$. Dimostriamo per induzione che $f_n(x) \in \mathbb{Z}[x]$, $f_n(x)$ primitivo e che $f_n(x)$ e' irriducibile in $\mathbb{Q}[x]$. Procediamo per induzione forte su n .

(3.1) $n = 1$

$$f(x) = x - 1 \Rightarrow f_1(x) = x - 1 \text{ che e' irriducibile in } \mathbb{Q}[x] \text{ ed e' anche primitivo}$$

(3.2) Supponiamo la tesi vera per $1 < m < n$ e dimostriamola per n

(3.2.1) $f_n(x) \in \mathbb{Z}[x]$ ed e' primitivo

Poiche' $n > 1$, l'insieme $\{m \nmid n, \ m \neq n\}$ non e' vuoto. Possiamo quindi considerare:

$$g(x) = \prod_{m \nmid n, \ m \neq n} f_m(x) \Rightarrow \exists m' < n : g(x) = \prod_{m \nmid m' \in \mathbb{Z}[x] \text{ per Hp indut.}} \underbrace{f_m(x)} \in \mathbb{Z}[x]$$

$$f_m(x) \text{ e' primitivo (per Hp indutt.) } \forall m < n \xRightarrow{\text{lemma di Gauss [AI,16.19,pg.69]}} \prod_{m \nmid m'} f_m(x) = g(x) \text{ e' primitivo (1)}$$

$$f(x) = f_n(x)g(x)$$

$$\begin{cases} f(x) \in \mathbb{Z}[x] \\ g(x) \in \mathbb{Z}[x] \end{cases} \Rightarrow f_n(x) = \frac{f(x)}{g(x)} \in \mathbb{Q}[x]$$

Con $c(f)$ indichiamo il contenuto del polinomio f (vedi [AI,16.2,pg.69]). Poiche' $f_n(x) \in$

$\mathbb{Q}[x]$, possiamo considerare la sua parte primitiva:

$$f(x) \in \mathbb{Q}[x] \Rightarrow f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_r}{b_r}x^r, \quad a_i, b_i \in \mathbb{Z}$$

$$f_n(x) = \frac{b}{d}\tilde{f}_n(x), \quad \text{dove}$$

$$d = \text{mcm} \{b_0, \dots, b_r\},$$

$$b = c(df(x)) = \text{MCD} \left\{ d \frac{a_i}{b_i} \mid i = 0, \dots, r \right\}$$

$$\tilde{f}_n(x) = \frac{da_0}{bb_0} + \frac{da_1}{bb_1}x + \cdots + \frac{da_r}{bb_r}x^r \in \mathbb{Z}[x]$$

$$\tilde{f}_n(x) \in \mathbb{Z}[x], \quad \tilde{f}_n(x) \text{ primitivo}$$

$$\tilde{f}_n(x) \text{ primitivo}, g(x) \text{ primitivo per la (1)} \quad \xRightarrow{\text{lemma Gauss [AI,16.19,pg.69]}} \quad \tilde{f}_n(x)g(x) \text{ primitivo} \Leftrightarrow c(\tilde{f}_ng) = 1$$

$$x^n - 1 = f(x) = f_n(x)g(x) = \frac{b}{d}\tilde{f}_n(x)g(x) \Rightarrow dx^n - d = b\tilde{f}_n(x)g(x) \Rightarrow$$

$$\Rightarrow \underbrace{c(dx^n - d)}_{=d} = c(b\tilde{f}_n(x)g(x)) \quad \underbrace{=}_{c(\tilde{f}_ng)=1} \quad b \Rightarrow b = d$$

$$f_n(x) = \frac{b}{d}\tilde{f}_n(x) \underbrace{=}_{d=b} \tilde{f}_n(x) \in \mathbb{Z}[x] \text{ ed e' primitivo}$$

(3.2.2) $f_n(x)$ e' irriducibile in $\mathbb{Q}[x]$

(3.2.2.1) Sia α radice di $f_n(x)$ e sia $p(x) = P_{\min}(\alpha, \mathbb{Q})$, si ha:

$$q \text{ primo t.c. } q \nmid n \Rightarrow p(\alpha^q) = 0$$

Infatti,

$$f_n(\alpha) = 0 \quad \xRightarrow{[2.28, \text{pg.23}]} \quad p(x) \mid f_n(x) \Leftrightarrow p(x)h(x) = f_n(x)$$

$$\begin{cases} (q, n) = 1 \\ U_n = \langle \alpha \rangle \end{cases} \Rightarrow \langle \alpha^q \rangle = U_n \Rightarrow f_n(\alpha^q) = 0 \Leftrightarrow p(\alpha^q)h(\alpha^q) = 0 \Leftrightarrow p(\alpha^q) = 0 \vee h(\alpha^q) = 0$$

Supponiamo per assurdo che $h(\alpha^q) = 0$

$$h(\alpha^q) = 0 \Rightarrow \alpha \text{ e' radice di } h(x^q) = 0 \quad \xRightarrow{[2.28, \text{pg.23}]} \quad p(x) \mid h(x^q) \Leftrightarrow p(x)l(x) = h(x^q)$$

Passando in $\mathbb{Z}_q[x]$, per la prop [1.20,pg.7] si ha :

$$p(x)l(x) = h(x)^q \quad \text{in } \mathbb{Z}_q[x] \quad (+)$$

Allora, preso un fattore irriducibile $p'(x) \in \mathbb{Z}_q[x]$ di $p(x)$, si ha

$$p'(x) \nmid p(x) \xRightarrow{(+)} p'(x) \nmid h(x)^q$$

$$p'(x) \text{ irriducibile in } \mathbb{Z}_q[x] \xLeftrightarrow[\mathbb{Z}_q[x] \text{ ED, [1.8,pg.2]}] p'(x) \text{ primo in } \mathbb{Z}_q[x]$$

$$\begin{cases} p'(x) \nmid h(x)^q \\ p'(x) \text{ primo} \end{cases} \Rightarrow p'(x) \nmid h(x) \text{ in } \mathbb{Z}_q[x] \Rightarrow p'(x)k(x) = h(x) \text{ in } \mathbb{Z}_q[x]$$

$$p'(x) \nmid p(x) \Rightarrow p(x) = p'(x)q'(x)$$

$$x^n - 1 = f(x) = f_n(x)g(x) = p(x)h(x)g(x) = p'(x)q'(x)p'(x)k(x)g(x) = p'(x)^2 q'(x)k(x)g(x)$$

$$p'(x)^2 \text{ ammette radici doppie} \Rightarrow x^n - 1 \text{ non e' separabile in } \mathbb{Z}_q[x]$$

$$D[x^n - 1] = nx^{n-1} \neq 0 \quad \forall x \neq 0$$

$$\underbrace{\quad}_{q \nmid n}$$

ma 0 non e' radice di $x^n - 1$

$$\Rightarrow \nexists \xi : \xi^n - 1 = 0 = D[x^n - 1](\xi) \Rightarrow$$

$$\xRightarrow{[1.17, \text{pg.6}]} x^n - 1 \text{ non ha radici mult. in } \mathbb{Z}_q[x] \Rightarrow x^n - 1 \text{ e' separabile in } \mathbb{Z}_q[x]$$

Assurdo.

$$(3.2.2.2) \quad f_n(x) \nmid p(x)$$

Sia γ una radice di $f_n(x)$. Per quanto visto in precedenza

$$\alpha \text{ radice di } f_n(x) \Rightarrow U_n = \langle \alpha \rangle \Rightarrow \exists i < n, (i, n) = 1 : \gamma = \alpha^i$$

$$i = p_1 \dots p_s \quad p_i \text{ primo}$$

$$(i, n) = 1 \Rightarrow p_i \nmid n \quad \forall i$$

$$\alpha^i = \alpha^{p_1 \dots p_s} = ((\alpha^{p_1})^{p_2}) \dots$$

Sia

$$\beta_k = (((\alpha^{p_1})^{p_2}) \dots)^{p_k}$$

dimostriamo per induzione che $f_n(\beta_k) = p(\beta_k) = 0 \quad \forall k = 1, \dots, s$:

1. Base:

$$\alpha \text{ radice di } f_n(x) \Rightarrow U_n = \langle \alpha \rangle$$

$$\begin{cases} (i, n) = 1 \\ p_1 \nmid i \end{cases} \Rightarrow (p_1, n) = 1$$

$$\xRightarrow{[AII, 1.45, \text{pg.16}]} U_n = \langle \alpha^{p_1} \rangle \Rightarrow \alpha^{p_1} = \beta_1 \text{ e' radice di } f_n(x)$$

$$p_1 \text{ primo, } p_1 \nmid n \xRightarrow{\text{passo 3.2.2.1}} p(\alpha^{p_1}) = 0 \Leftrightarrow p(\beta_1) = 0$$

2.

$$\beta_{k+1} = \beta_k^{p_{k+1}}$$

Per l'Hp induttiva, β_k e' una radice di $f_n(x)$, allora applicando la base (sostituendo α con β_k e p_1 con p_{k+1}) si ha $f_n(\beta_{k+1}) = 0$,

Per Hp induttiva $p(\beta_k) = 0 \Rightarrow p(x) = P_{\min}(\beta_k, \mathbb{Q})$

$$\begin{cases} f_n(\beta_k) = 0 \\ p(x) = P_{\min}(\beta_k, \mathbb{Q}) \\ p_{k+1} \nmid n \end{cases} \quad \underbrace{\Rightarrow}_{\text{passo 3.2.2.1}} \quad p(\beta_k^{p_{k+1}}) = 0 \Leftrightarrow p(\beta_{k+1}) = 0$$

In particolare, per $k = s$, abbiamo

$$\beta_s = \alpha^{p_1 \cdots p_s} = \alpha^i = \gamma$$

$$p(\beta_s) = 0 \Leftrightarrow p(\alpha^i) = 0 \Leftrightarrow p(\gamma) = 0$$

Ricapitolando: abbiamo preso una generica radice γ di $f_n(x)$ e visto che $p(\gamma) = 0$ quindi, per Ruffini

$$f_n(x) / p(x)$$

e poiche' avevamo gia' visto che $p(x) / f_n(x)$, si ha $f_n(x) = p(x)$. Quindi

$$f_n(x) = p(x) = P_{\min}(\alpha, \mathbb{Q}) \Rightarrow f(x) \text{ irriducibile in } \mathbb{Q}[x]$$

(3.2.3) Q.E.D.

$$\begin{cases} f_n(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x] \\ f_n(x) \text{ irriducibile in } \mathbb{Q}[x] \\ f_n(x) \text{ monico} \\ f_n(\omega) = 0 \end{cases} \quad \underbrace{\Rightarrow}_{[2.30, \text{pg.24}]} \quad f_n(x) = P_{\min}(\omega, \mathbb{Q})$$

che e' la tesi dell'induzione.

(4) Dim 3.

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg P_{\min}(\omega, \mathbb{Q}) = \deg f_n(x) \quad \underbrace{=}_{\text{passo 2}} \quad \varphi(n)$$

(5) Dim 4.

$$CS(f_n(x), \mathbb{Q}) = \mathbb{Q}(\omega)$$

Per costruzione $f_n(x)$ e' separabile

$$\underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} \quad \mathbb{Q} \preceq \mathbb{Q}(\omega) \text{ e' di Galois}$$

□

Proposition 6.43. Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unita' e sia $(U(\mathbb{Z}_n), \cdot)$ il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_n$. Si ha

$$\mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \simeq U(\mathbb{Z}_n)$$

Proof: Per il thm [6.42, pg.114], $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ e' di Galois.

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega) \text{ Galois} \quad \underbrace{\Rightarrow}_{[6.24, \text{pg.96}]} \quad \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) = \mathcal{I}(\mathbb{Q}(\omega), \mathbb{Q})$$

Possiamo quindi usare la prop [6.8,pg.81] per determinare gli elementi di $\mathcal{I}(\mathbb{Q}(\omega), \mathbb{Q})$. Sempre per il thm [6.42,pg.114], si ha

$$P_{\min}(\omega, \mathbb{Q}) = f_n(x)$$

le radici di $f_n(x)$ sono $\{u \in U_n \mid U_n = \langle u \rangle, \}$ $\underbrace{=}_{U_n = \langle \omega \rangle} \{\omega^i \in U_n \mid U_n = \langle \omega^i \rangle, 0 \leq i \leq n-1\} =$

$$\underbrace{=}_{[AII, 1.45, pg.16]} \{u^i \in U_n \mid (i, n) = 1, 0 \leq i \leq n-1\}$$

[AII, 1.45, pg.16]

quindi gli elementi di $\mathcal{I}(\mathbb{Q}(\omega), \mathbb{Q})$ sono determinati dalle seguenti assegnazioni:

$$\omega \xrightarrow{\psi_i} \omega^i, \quad \text{con } (i, n) = 1$$

Ricordando che

$$U(\mathbb{Z}_n) = \{z \in \mathbb{Z}_n \mid \exists z^{-1}\} \underbrace{=}_{[AI, 10.1, pg.45]} \{z \in \mathbb{Z}_n \mid (z, n) = 1\}$$

scegliamo quindi la seguente mappa:

$$\begin{aligned} \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) &\longrightarrow U(\mathbb{Z}_n) \\ \psi_i &\xrightarrow{\Phi} i \end{aligned}$$

(1) Φ e' iniettiva

$$\begin{aligned} \Phi(\psi_i) = \Phi(\psi_j) &\Leftrightarrow i = j \\ \left\{ \begin{array}{l} \psi_i(\omega) = \omega^i \underbrace{=}_{i=j} \omega^j = \psi_j(\omega) \\ \psi_i, \psi_j \in \mathcal{I}(\mathbb{Q}(\omega), \mathbb{Q}) \end{array} \right. &\xRightarrow{[6.8, pg.81]} \psi_i = \psi_j \end{aligned}$$

(2) Φ e' surriettiva

$$\begin{aligned} \mathbb{Q} \subseteq \mathbb{Q}(\omega) \text{ di Galois} &\xRightarrow{[6.19, pg.92]} |\mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] \underbrace{=}_{[6.42, pg.114]} \psi(n) \\ |U(\mathbb{Z}_n)| &\underbrace{=}_{[AI, 12.1, pg.54]} \psi(n) \end{aligned}$$

$$\left\{ \begin{array}{l} \Phi : \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \longrightarrow U(\mathbb{Z}_n) \text{ iniettiva} \\ |U(\mathbb{Z}_n)| = |\mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q})| \end{array} \right. \Rightarrow \Phi \text{ surriettiva}$$

(3) Φ e' un omomorfismo di gruppi

$$\begin{aligned} \varphi_i \varphi_j(\omega) &= \varphi_i(\omega^j) = \varphi_i(\omega)^j = (\omega^i)^j = \omega^{ij} \\ \Phi(\varphi_i \varphi_j) &= ij \\ \Phi(\varphi_i) \Phi(\varphi_j) &= ij \end{aligned}$$

□

6.3 Riga e compasso

Definition 6.44. Sia $\mathbf{E} = \mathbb{R}^2$ il piano affine euclideo costruito sullo spazio vettoriale $\mathbb{R}^2$ (nota²¹)

Una costruzione euclidea (con riga e compasso) e' una successione $A_0, \dots, A_n$ di punti, rette

²¹e' in pratica l'usuale piano $\mathbb{R}^2$ dotato di prodotto scalare e quindi di norma, distanza, angoli. Vedi [GII, 3, pg.56]

e circonferenze, tali che

1. $A_0, A_1 \in \mathbf{E}$, ovvero sono due punti del piano
2. A_i e' una retta $\Rightarrow \exists j, k < i : A_j, A_k \in \mathbf{E}, \overline{A_j A_k} = A_i$
dove $\overline{A_j A_k}$ e' la retta passante per i punti A_j, A_k
3. A_i e' una circonferenza $\Rightarrow \exists h, j, k < i : A_h, A_j, A_k \in \mathbf{E}, \mathcal{C}(A_h, \|\overrightarrow{A_j A_k}\|) = A_i$
dove $\overrightarrow{A_j A_k}$ e' il vettore $A_k - A_j$
 $\|\overrightarrow{A_j A_k}\|$ e' la sua norma
 $\mathcal{C}(A_h, \|\overrightarrow{A_j A_k}\|)$ e' la circonferenza di centro A_h e raggio $\|\overrightarrow{A_j A_k}\|$
4. $A_i \in \mathbf{E} \Rightarrow \exists j, k < i : A_i, A_j \subseteq \mathbf{E}, A_i \in A_j \cap A_k, |A_j \cap A_k| < +\infty$

In pratica, ogni passo della costruzione deve essere realizzato mediante elementi a lui precedenti, gia' costruiti. Gli unici due punti arbitrari sono quelli iniziali A_0, A_1 , tutti gli altri si devono ricavare tramite intersezioni di oggetti costruiti.

Definition 6.45.

$a \in \mathbb{R}$ e' un numero euclideo $\stackrel{\text{def}}{\Leftrightarrow} \exists A$ costruzione euclidea t.c. $\exists i, j : A_i, A_j \in \mathbf{E}, \|\overrightarrow{A_i A_j}\| = |a|$
 $a + ib \in \mathbb{C}$ e' un numero euclideo $\stackrel{\text{def}}{\Leftrightarrow} a, b \in \mathbb{R}$ sono euclidei

Poniamo

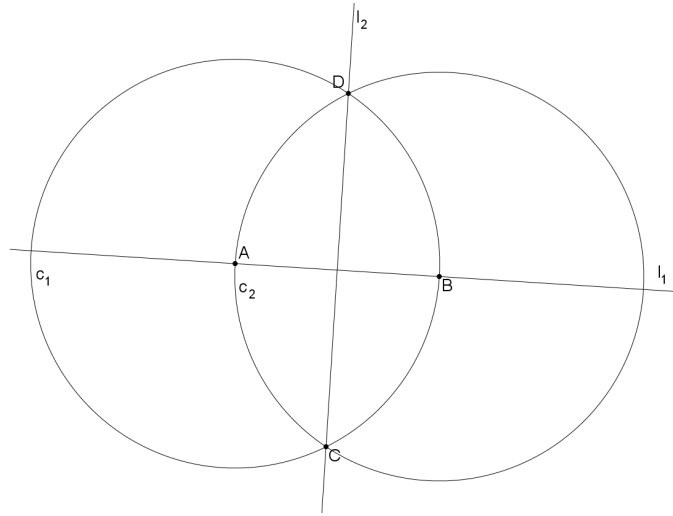
$$\mathbf{E} = \{a \in \mathbb{R} \mid a \text{ e' euclideo}\} \cup \{1\}$$

Proposition 6.46. *Esistono le seguenti costruzioni:*

1. *Asse del segmento $A_0 A_1$. Lo indicheremo con $\text{Asse}(A_0, A_1)$.*
2. *Retta r perpendicolare a una retta s e passante per un punto P . La indicheremo con $r = \text{Perp}(s, P)$.*
3. *Retta r parallela a s passante per P . La indicheremo con $r = \text{Parall}(s, P)$.*
4. *Segmento di lunghezza l su una retta r usando come estremo un punto $P \in r$*

Proof:

(1) Dim. 1.



Dove

$$A_0 = A$$

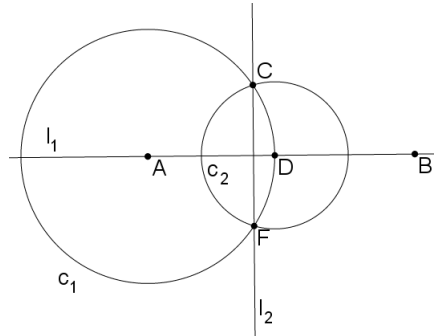
$$A_1 = B$$

$$A_2 = c_1 = \mathcal{C}(A, \|\overrightarrow{AB}\|)$$

$$A_3 = c_2 = \mathcal{C}(B, \|\overrightarrow{AB}\|)$$

$$A_4 = D \in c_1 \cap c_2$$

A_4 e' l'asse cercato, lo indicheremo con $A_4 = \text{Asse}(A, B)$.
 (2) Dim 2.



Dove

$$A_0 = A$$

$$A_1 = B$$

$$A_2 = s = l_1 = \overline{AB} \text{ la retta data}$$

$$C = P \text{ e' il punto dato}$$

$$A_4 = c_1 = \mathcal{C}(A, \|\overrightarrow{AC}\|)$$

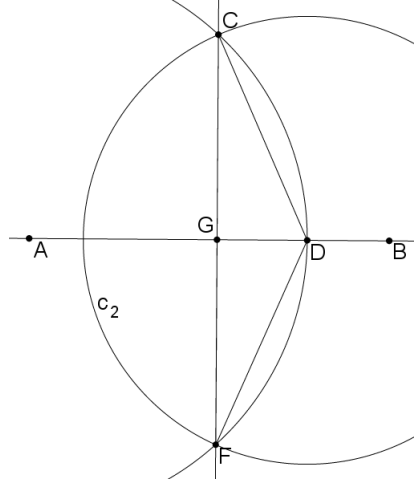
$$A_5 = D \in c_1 \cap s$$

$$A_6 = c_2 = \mathcal{C}(D, \|\overrightarrow{DC}\|)$$

$$A_7 = F \in c_2 \cap c_1$$

$$A_8 = \overline{CF}$$

⟨2.1⟩ Dimostriamo che A_8 e' la retta perpendicolare a s in C . Ovvero, $A_8 = \text{Perp}(s, C)$



Abbiamo

$$\|\vec{DF}\| = \|\vec{DC}\| = \text{raggio di } c_2$$

$$\Rightarrow \text{il triangolo } DCF \text{ e' isoscele} \Rightarrow \underbrace{D\hat{C}F = D\hat{F}C}_{\text{angoli alla base del triangolo isoscele}} \quad (1)$$

$$\|\vec{AC}\| = \|\vec{AD}\| = \|\vec{AF}\| = \text{raggio di } c_1$$

$$\Rightarrow \text{i triangoli } ACD, ADF, ACF \text{ sono isosceli} \Rightarrow \begin{cases} A\hat{C}D = C\hat{D}A \\ A\hat{D}F = D\hat{F}A \\ A\hat{C}F = C\hat{F}A \end{cases} \quad (2)$$

$$\begin{cases} A\hat{C}D = A\hat{C}F + C\hat{F}D \\ A\hat{F}D = A\hat{F}C + C\hat{F}D \end{cases} \quad (3)$$

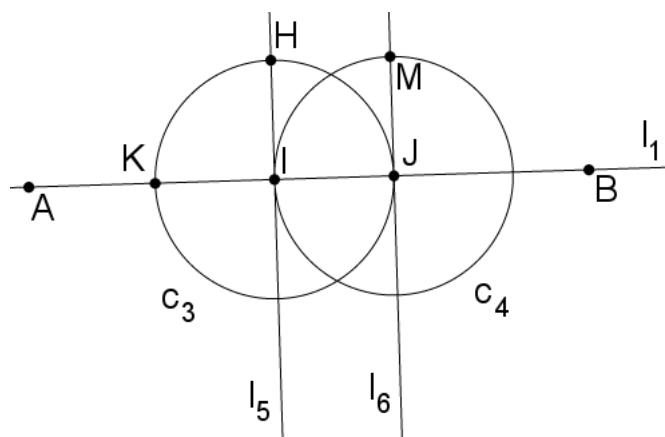
$$\begin{cases} C\hat{D}A \underset{(2)}{=} A\hat{C}D \underset{(3)}{=} A\hat{C}F + C\hat{F}D \\ A\hat{D}F \underset{(2)}{=} D\hat{F}A \underset{(3)}{=} A\hat{F}C + C\hat{F}D \underset{(2)}{=} A\hat{C}F + C\hat{F}D \end{cases} \Rightarrow A\hat{D}F = C\hat{D}A \Leftrightarrow G\hat{D}F = C\hat{D}G \quad (4)$$

$$(1) \Rightarrow D\hat{F}G = D\hat{C}G \quad (1.1)$$

$$\begin{cases} C\hat{G}D = \pi - G\hat{C}D - C\hat{D}G \\ D\hat{G}F = \pi - G\hat{D}F - D\hat{F}G \end{cases} \underset{(4), (1.1)}{\Rightarrow} C\hat{G}D = D\hat{G}F$$

$$\begin{cases} C\hat{G}D = D\hat{G}F \\ C\hat{G}D + D\hat{G}F \end{cases} \underset{C, G, F \text{ sono allineati}}{=} \pi \Rightarrow C\hat{G}D = D\hat{G}F = \frac{\pi}{2}$$

⟨3⟩ Dim 3.



Dove

$$A_0 = A$$

$$A_1 = B$$

$$A_2 = s = l_1 = \overline{AB} \text{ la retta data}$$

$$H = P \text{ e' il punto dato}$$

$$A_3 = l_5 = \text{Perp}(\overline{AB}, H)$$

$$A_4 = I \in A_3 \cap \overline{AB}$$

$$A_5 = c_3 = \mathcal{C}(I, \|\vec{IH}\|)$$

$$A_6 = J \in c_3 \cap \overline{AB}$$

$$A_7 = c_4 = \mathcal{C}(J, \|\vec{JI}\|)$$

$$A_8 = l_6 = \text{Perp}(\overline{AB}, J)$$

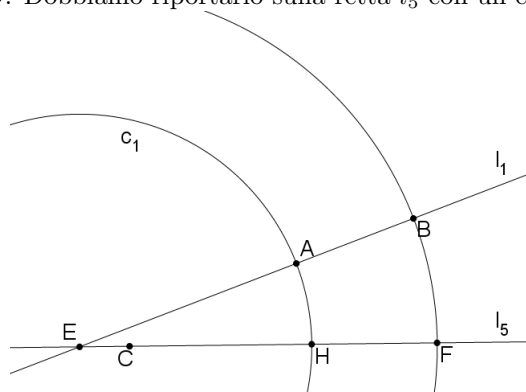
$$A_9 = M \in c_4 \cap A_8$$

$$A_{10} = \overline{HM}$$

A_{10} e' la retta parallela a s passante per H .

(4) Dim 4.

E' dato il segmento AB . Dobbiamo riportarlo sulla retta l_5 con un estremo in L .



Prima di tutto riportiamo HF su $\overline{AB}$ senza curarci di L .

$$A_0 = A$$

$$A_1 = B$$

$$A_2 = l_1 = \overline{AB}$$

$$A_3 = E \in \overline{AB} \cap l_5$$

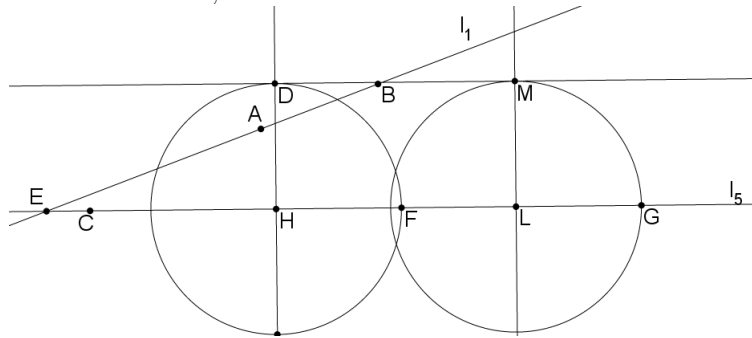
$$A_4 = c_1 = \mathcal{C}(E, \|\overrightarrow{EA}\|)$$

$$A_5 = c_2 = \mathcal{C}(E, \|\overrightarrow{EB}\|)$$

$$A_6 = H \in c_1 \cap l_5$$

$$A_7 = F \in c_2 \cap l_5$$

Adesso spostiamo HF a destra, facendo diventare L un estremo.



$$A_8 = \text{Perp}(l_5, H)$$

$$A_9 = c_3 = \mathcal{C}(H, \|\overrightarrow{HF}\|)$$

$$A_{10} = D \in c_3 \cap A_8$$

$$A_{11} = \text{Parall}(l_5, D)$$

$$A_{12} = \text{Perp}(l_5, L)$$

$$A_{13} = M \in A_{11} \cap A_{12}$$

$$A_{14} = c_4 = \mathcal{C}(L, \|\overrightarrow{LM}\|)$$

$$A_{15} = G \in c_4 \cap l_5$$

LG e' il segmento cercato.

□

Proposition 6.47.

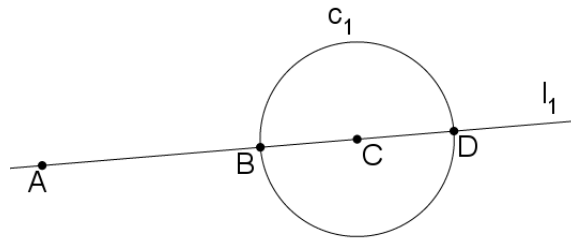
$$a, b, c \in \mathbb{E}, c \neq 0 \Rightarrow b \pm a, ab, ac^{-1}, \sqrt{|a|} \in \mathbb{E}$$

Proof:

(1) Dim $b \pm a \in \mathbb{E}$

Per Hp a, b sono euclidei, quindi riusciamo a costruire dei segmenti che hanno modulo $|a|, |b|$.

Per la prop [6.46,pg.120] riusciamo anche a riportare tali segmenti sulla retta $\overline{A_0A_1}$ in modo che il loro primo estremo sia A_0 . Vedi figura:



dove

$$\begin{aligned}
 A_0 &= A \\
 A_2 &= l_1 = \overline{A_0 A_1} \\
 \|\overrightarrow{AB}\| &= a \\
 \|\overrightarrow{AC}\| &= b \\
 A_3 &= c_1 = \mathcal{C}(C, \|\overrightarrow{CB}\|) \\
 A_4 &= D \in c_1 \cap l_1
 \end{aligned}$$

Quindi

$$\|\overrightarrow{AB}\| = b - a$$

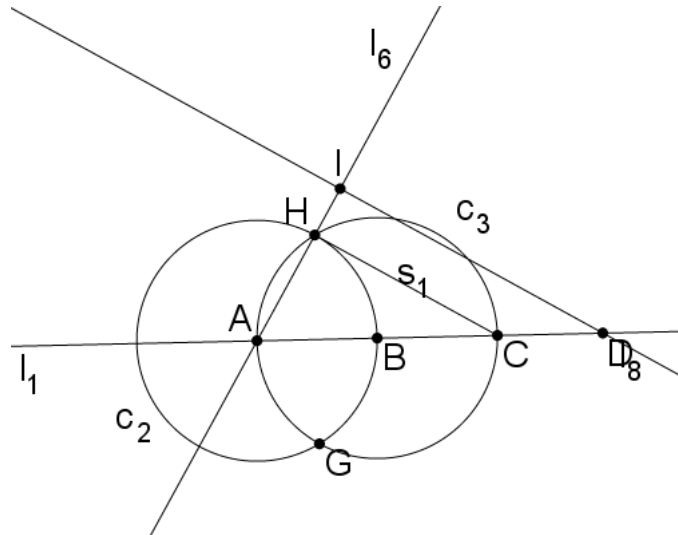
Per la somma riportiamo AB sulla stessa retta l_1 con C come estremo sinistro (basta usare la prop [6.46,pg.120]).

(2) $ab, ac^{-1} \in \mathbb{E}$

Per definizione $1 \in \mathbb{E}$. E' allora costruibile un segmento AB di lunghezza 1.

Poiche' $c \in \mathbb{E}$, per la prop [6.46,pg.120], possiamo costruire su $\overline{AB}$ il segmento AC , con $\|\overrightarrow{AC}\| = c$.

Per il passo precedente, $a+c \in \mathbb{E}$, quindi possiamo costruire il segmento AD , con $\|\overrightarrow{AD}\| = a+c$. Allora



dove

$$c_2 = \mathcal{C}(A, \|\overrightarrow{AB}\|)$$

$$c_3 = \mathcal{C}(B, \|\overrightarrow{BA}\|)$$

$$H \in c_2 \cap c_3$$

$$l_6 = \overline{AH}$$

$$s_1 = \overline{HC}$$

$$l_8 = \text{Parall}(\overline{HC}, D)$$

$$I \in l_8 \cap l_6$$

Abbiamo:

$$\|\overrightarrow{AH}\| = \|\overrightarrow{AB}\| = 1$$

$$\|\overrightarrow{CD}\| = \|\overrightarrow{AD}\| - \|\overrightarrow{AC}\| = a$$

Per il thm di Talete, abbiamo:

$$\|\overrightarrow{AH}\| : \|\overrightarrow{AC}\| = \|\overrightarrow{HL}\| : \|\overrightarrow{CD}\| \Leftrightarrow 1 : c = \|\overrightarrow{HL}\| : a \Leftrightarrow \|\overrightarrow{HL}\| = \frac{a}{c} = ac^{-1}$$

Per il prodotto: invece di riportare $a + c$ su AD , riportiamo a su HL , cioè' $\|\overrightarrow{HL}\| = a$, avremo così':

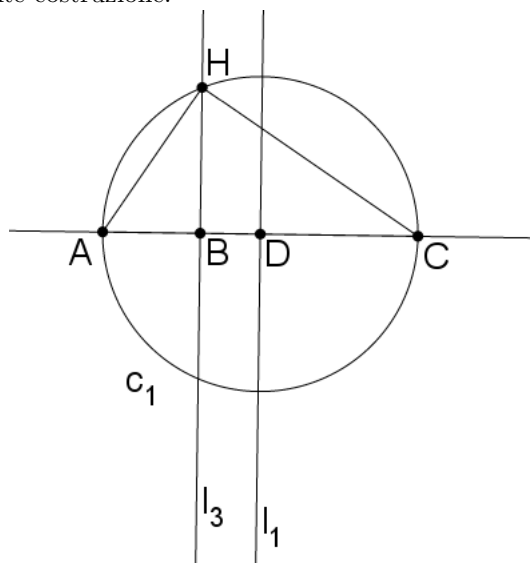
$$l_8 = \text{Parall}(\overline{HC}, I)$$

$$D \in l_8 \cap l_1$$

$$\|\overrightarrow{AH}\| : \|\overrightarrow{AC}\| = \|\overrightarrow{HL}\| : \|\overrightarrow{CD}\| \Leftrightarrow 1 : c = a : \|\overrightarrow{CD}\| \Leftrightarrow \|\overrightarrow{CD}\| = ac$$

(3) $\sqrt{a} \in \mathbb{E}$, con $a \geq 0$

Consideriamo la seguente costruzione:



dove

Costruiamo $\overline{AB}$

Riportiamo a su BC usando la prop [6.46,pg.120]

$l_1 = \text{Asse}(A, C)$

$D \in l_1 \cap \overline{AB}$

$c_1 = \mathcal{C}(D, \|\overrightarrow{DA}\|)$

Per il secondo teorema di Euclide:

$$\|\overrightarrow{AB}\| : \|\overrightarrow{BH}\| = \|\overrightarrow{BH}\| : \|\overrightarrow{BC}\|$$

basta allora scegliere

$$\|\overrightarrow{AB}\| = 1$$

$$\|\overrightarrow{BC}\| = a$$

per avere

$$1 : \|\overrightarrow{BH}\| = \|\overrightarrow{BH}\| : a \Leftrightarrow \|\overrightarrow{BH}\|^2 = a \Leftrightarrow \|\overrightarrow{BH}\| = \sqrt{a}$$

□

Proposition 6.48.

$$\mathbb{Q} \leq \mathbb{E} \leq \mathbb{R}$$

Proof: Per definizione $\mathbb{E} \subseteq \mathbb{R}$. E' anche un sottocampo: basta applicare la prop [1.6,pg.1] e la prop [6.47,pg.124].

Infine, poiche' $\mathbb{E}$ e' un sottocampo di $\mathbb{R}$:

$$\text{ch}\mathbb{E} \underbrace{=}_{[2.8, \text{pg.12}]} \text{ch}\mathbb{R} = 0 \underbrace{\Rightarrow}_{[2.9, \text{pg.13}]} \mathbb{Q} \hookrightarrow K$$

□

Proposition 6.49. Posto $\mathbf{F} = \mathbb{E}^2$, $A_0 = O = (0, 0)$, $A_1 = (1, 0)$, si ha

1. Le seguenti mappe rendono $\mathbf{F}$ uno spazio affine euclideo sullo spazio vettoriale $\mathbb{E}^2$

$$\overrightarrow{PQ} = Q - P \quad \forall P, Q \in \mathbf{F}$$

$$(x, y) \cdot (x', y') = xx' + yy' \quad \forall x, y, x', y' \in \mathbb{E}$$

2. $\mathbf{F} = \{P \in \mathbf{E} \mid P \text{ e' costruibile a partire da } A_0, A_1\}$

La 2. si puo' interpretare cosi': l'insiemi dei punti del piano con coordinate euclidee e' uguale all'insieme dei punti costruibili del piano.

Nota: da ora in poi supporremo $A_0 = O = (0, 0)$, $A_1 = (1, 0)$.

Proof: Per la prop [6.48,pg.127] $\mathbb{E}$ e' un campo. Possiamo quindi considerare lo spazio affine euclideo $\mathbf{F}$ sullo spazio vettoriale $\mathbb{E}^2$:

$$\mathbf{F} = \mathbb{E}^2$$

$$\overrightarrow{PQ} = Q - P \quad \forall P, Q \in \mathbf{F}$$

$$(x, y) \cdot (x', y') = xx' + yy' \quad \forall x, y, x', y' \in \mathbb{E}$$

Scelto un riferimento $(O, \{\vec{X}, \vec{Y}\})$, $O \in \mathbf{F}$, $\vec{X}, \vec{Y} \in \mathbb{E}^2$, a ogni punto $P \in \mathbf{F}$ possiamo associare le sue coordinate $[P]$. Scegliendo il riferimento canonico $O = (0, 0)$, $\vec{X} = (1, 0)$, $\vec{Y} = (0, 1)$, abbiamo

$$[P] = P$$

(Nota²²)

(1) Fissati $A_0 = O = (0, 0)$, $A_1 = (1, 0)$, dimostriamo che

$$\mathbf{F} = \{P \in \mathbf{E} \mid P \text{ e' costruibile a partire da } A_0, A_1\}$$

(1.1) $\subseteq$

Costruiamo gli assi X e Y :

$$X = \overline{A_0 A_1}$$

$$Y = \text{Perp}(X, A_0)$$

Abbiamo:

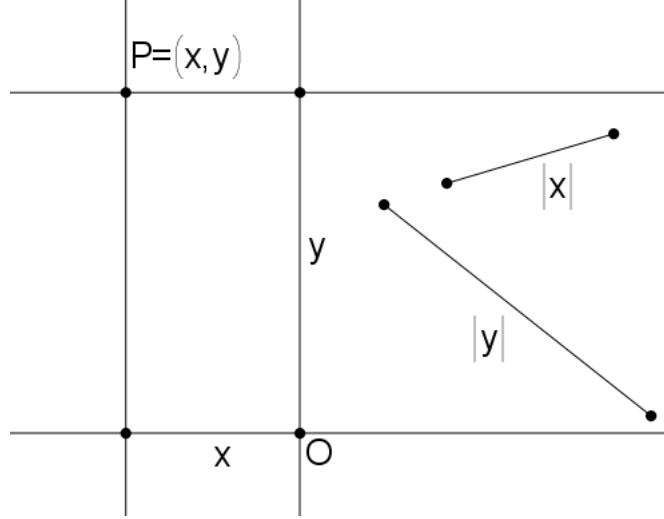
$$P = (x, y) \in \mathbf{F} = \mathbb{E}^2 \Rightarrow x, y \in \mathbb{E} \Rightarrow \exists i, j, h, k : A_i, A_j, A_h, A_k \in \mathbf{E}, \quad \|\overrightarrow{A_i A_j}\| = |x|, \quad \|\overrightarrow{A_h A_k}\| = |y|$$

Riportiamo i segmenti $A_i A_j$, $A_h A_k$ rispettivamente sull'asse X e Y usando O come primo estremo (vedi [6.46, pg. 120]) e scegliendo il secondo estremo in modo da rispettare il segno di x e y .

Dai secondi estremi tracciamo la perpendicolare agli assi e intersechiamo le rette ottenute.

Il punto d'intersezione avr  coordinate (x, y) .

Abbiamo cos  costruito il punto P a partire da A_0, A_1 . Poich  $P \in \mathbf{F} = \mathbb{E}^2 \subseteq \mathbb{R}^2 = \mathbf{E}$, si ha che P appartiene al secondo insieme.



(1.2) $\supseteq$

Sia $P \in \{P \in \mathbf{E} \mid P \text{ e' costruibile a partire da } A_0, A_1\}$. Quindi $\exists i : A_i = P$.

Costruiamo gli assi X, Y come prima, e tracciamo la perpendicolare ad essi passante per P .

Intersecando X, Y con tali perpendicolari otteniamo i punti Q, R . Quindi,

$$P = (\pm \|\overrightarrow{OQ}\|, \pm \|\overrightarrow{OR}\|)$$

dove i segni devono essere scelti in maniera opportuna. Le coordinate di P sono quindi dei numeri euclidei: $P \in \mathbb{E}^2 = \mathbf{F}$.

□

Theorem 6.50.

$$a \in \mathbb{E} \Leftrightarrow \exists \text{ una catena di campi } \mathbb{Q} = K_0 \preceq K_1 \preceq \dots \preceq K_t \preceq \mathbb{R} \text{ tale che } \begin{cases} a \in K_t \\ t \geq 1 \Rightarrow [K_i : K_{i-1}] = 2 \quad \forall i = 1, \dots, t \end{cases}$$

Proof:

²²anche se $\mathbb{E}^2 \subseteq \mathbb{R}^2$, non e' vero che $\mathbf{F} = \mathbb{E}^2$ e' un sottospazio vettoriale di $\mathbf{E} = \mathbb{R}^2$, infatti il primo e' uno spazio costruito sul campo $\mathbb{E}$, il secondo e' invece costruito su $\mathbb{R}$ e come vedremo $\mathbb{E} \subsetneq \mathbb{R}$

(1) Dim. $\Rightarrow$

Sia $a \in \mathbb{E}$ e $P = (a, 0) \in \mathbb{E}^2 = \mathbf{F}$. Per la prop [6.49,pg.127] P e' costruibile a partire da A_0, A_1 , ovvero

$$\exists A_2, A_3, \dots, A_m \text{ costruzione euclidea t.c. } A_m = P$$

Siano $P_0, \dots, P_s$ tutti i punti che compaiono nella costruzione, con

$$P_0 = A_0, P_1 = A_1$$

$$P_{s-1} = A_j, \quad j < m, \quad P_s = A_m = P$$

$A_{j+1}, A_{j+2}, \dots, A_{m-1}$ sono le rette e circonferenze costruite dopo P_{s-1} e prima di P_s

(1.1) Dimostriamo per induzione su s che

$$\exists \mathbb{Q} = K_0 \preceq K_1 \preceq \dots \preceq K_t \preceq \mathbb{R} \text{ tale che } \begin{cases} (P_i)_1, (P_i)_2 \in K_t \\ t \geq 1 \Rightarrow [K_h : K_{h-1}] = 2 \quad \forall h = 1, \dots, t \end{cases} \quad \forall i = 0, 1, \dots, s$$

Nota: $(P_i)_1$ e' la prima coordinata del punto P_i , cioe' $P_i = ((P_i)_1, (P_i)_2)$

Per $s = 1$, si ha

$$P_s = P_1 = A_1 = (1, 0) \in \mathbb{Q}^2 = K_0^2$$

$$P_0 = A_0 = O = (0, 0) \in \mathbb{Q}^2 = K_0^2$$

quindi la tesi e' vera con $t = 0$.

Supponendo la tesi vera per $s - 1$, si ha

$$\exists \mathbb{Q} = K_0 \preceq K_1 \preceq \dots \preceq K_t \preceq \mathbb{R} \text{ tale che } \begin{cases} (P_i)_1, (P_i)_2 \in K_t \\ t \geq 1 \Rightarrow [K_h : K_{h-1}] = 2 \quad \forall h = 1, \dots, t \end{cases} \quad \forall i = 0, 1, \dots, s - 1$$

Le rette e circonferenze della costruzione sono state ricavate dai punti $P_0, \dots, P_{s-1}$, che hanno le coordinate in K_t . Allora, le equazioni di tali rette e circonferenze saranno dei polinomi in $K_t[X, Y]$. Ad esempio, la circonferenza $\mathcal{C}(P_2, \|\vec{P_2 P_3}\|)$ e' descritta dall'equazione:

$$\underbrace{(X - (P_2)_1)^2 + (Y - (P_2)_2)^2 - \|\vec{P_2 P_3}\|^2}_{\in K_t[x]} = 0$$

Il punto $P_s = (x_s, y_s)$ e' intersezione di due rette o di due circonferenze o di una retta e circonferenza. Le equazioni di tali curve sono di grado ≤ 2 e in $K_t[X, Y]$. Analizziamo il terzo caso: P_s e' dato dalla soluzione di un sistema del tipo:

$$a, b, c, d \in K_t$$

$$\begin{cases} (X - a)^2 + (Y - b)^2 - r^2 = 0 \\ (X - c)^2 + (Y - d)^2 - r^2 = 0 \end{cases} \Leftrightarrow \begin{cases} X^2 - 2Xa + a^2 + Y^2 - 2Yb + b^2 - r^2 = 0 \\ X^2 - 2Xc + c^2 + Y^2 - 2dY + d^2 - r^2 = 0 \end{cases} \quad \begin{matrix} \Leftrightarrow \\ \text{sottraendo membro a membro} \end{matrix}$$

$$\Leftrightarrow \begin{cases} (-2a + 2c)X + (2d - 2b)Y + a^2 - d^2 + b^2 - c^2 = 0 \\ X^2 - 2cX + c^2 + Y^2 - 2dY + d^2 - r^2 = 0 \end{cases}$$

ci siamo cosi' ricondotti all'intersezione retta-circonferenza, cioe' a un sistema del tipo:

$$a, b, c, d, e \in K_t \begin{cases} aX + bY + c = 0 \\ (X - d)^2 + (Y - e)^2 - r^2 = 0 \end{cases}$$

Ricavando la X o la Y dalla prima equazione e sostituendo nella seconda, arriviamo a un'equazione di secondo grado. Le sue radici saranno del tipo

$$b, \Delta \in K_t$$

$$X = \frac{-b \pm \sqrt{\Delta}}{2} \in K_t(\sqrt{\Delta}) \quad (1)$$

Si ha

$$\Delta \in K_t \Rightarrow x^2 - \Delta \in K_t[x]$$

$$\sqrt{\Delta} \text{ e' radice di } x^2 - \Delta \quad (2)$$

$$\Rightarrow \sqrt{\Delta} \text{ e' algebrico su } K_t \quad \underbrace{\Rightarrow}_{[2.28, \text{pg. 23}]} \exists p(x) = P_{\min}(\sqrt{\Delta}, K_t)$$

$$(2) \Rightarrow p(x) / x^2 - \Delta \Rightarrow \deg p(x) \leq 2$$

Si possono verificare due casi:

CASE: $\deg p(x) = 1$

Quindi

$$p(x) = x - \sqrt{\Delta} \in K_t[x] \Rightarrow \sqrt{\Delta} \in K_t \Rightarrow K_t(\sqrt{\Delta}) = K_t$$

$$X \underbrace{\in}_{(1)} K_t(\sqrt{\Delta}) = K_t \Rightarrow Y \in K_t$$

Ma X, Y sono le coordinate di P_s , quindi la catena cercata e' sempre
 $K_0 \preceq \dots \preceq K_t$

CASE: $\deg p(x) = 2$

$$\deg p(x) = 2 \Rightarrow [K_t(\sqrt{\Delta}) : K_t] = 2$$

Quindi la catena cercata e'

$$K_0 \preceq \dots \preceq K_t \preceq K_t(\sqrt{\Delta})$$

(1) Dim. $\Leftarrow$

Data la solita catena $\mathbb{Q} = K_0 \preceq \dots \preceq K_t$, supponendo che $a \in K_t$, dimostriamo che $a \in \mathbb{E}$, ovvero che $K_t \subseteq \mathbb{E}$.

(1.1) Procediamo induzione su t .

Per $t = 0$

$$K_0 = \mathbb{Q} \quad \underbrace{\subseteq}_{[6.48, \text{pg. 127}]} \mathbb{E}$$

Passo induttivo, con $t \geq 1$.

Poiche' per Hp induttiva $K_{t-1} \subseteq \mathbb{E}$, basta dimostrare che $K_t \setminus K_{t-1} \subseteq \mathbb{E}$

Sia $a \in K_t \setminus K_{t-1}$

$$\Rightarrow K_{t-1} \subsetneq K_{t-1}(a) \subseteq K_t \Rightarrow 1 < [K_{t-1}(a) : K_{t-1}] \leq [K_t : K_{t-1}] \quad \underbrace{=}_{\text{Per Hp}} 2 \Rightarrow [K_{t-1}(a) : K_{t-1}] = 2$$

$$\underbrace{\Rightarrow}_{[2.18, \text{pg. 16}]} [K_t : K_{t-1}(a) = 1] \Rightarrow K_t = K_{t-1}(a) \quad (3)$$

$$[K_t : K_{t-1}] = 2 \Rightarrow K_{t-1} \subseteq K_t \text{ finita} \Rightarrow$$

$$\Rightarrow K_{t-1} \subseteq K_t \text{ algebrica } a \in K_t \text{ e' algebrico su } K_{t-1} \Rightarrow \exists p(x) = P_{\min}(a, K_{t-1})$$

$$\deg p(x) = [K_{t-1}(a) : K_{t-1}] \underbrace{=}_{(3)} [K_t : K_{t-1}] = 2 \Rightarrow p(x) = cx^2 + dx + e, \quad c, d, e \in K_{t-1}$$

$$p(a) = 0 \Rightarrow a = \frac{-d \pm \sqrt{d^2 - 4ce}}{2}$$

$$a \in \mathbb{K}_t \subseteq \mathbb{R} \Rightarrow d^2 - 4ce \geq 0$$

$$c, d, e \in K_{t-1} \subseteq \mathbb{E} \quad \underbrace{\Rightarrow}_{\mathbb{E} \text{ campo}} d^2 - 4ce \in \mathbb{E} \quad \underbrace{\Rightarrow}_{d^2 - 4ce \geq 0, [6.47, \text{pg. 124}]} \sqrt{d^2 - 4ce} \in \mathbb{E} \quad \underbrace{\Rightarrow}_{\mathbb{E} \text{ campo}} \frac{-d \pm \sqrt{d^2 - 4ce}}{2} = a \in \mathbb{E}$$

Quindi $a \in \mathbb{E}$, cioè la tesi. □

Corollary 6.51.

$$a \in \mathbb{E} \Rightarrow a \text{ e' algebrico su } \mathbb{Q}, \quad \deg P_{\min}(a, \mathbb{Q}) = 2^m, \quad m \geq 0$$

Proof: Per il thm [6.50,pg.128] abbiamo

$$a \in K_t \succeq \dots \succeq K_0 = \mathbb{Q}$$

Se $t = 0$ allora $a \in K_0 = \mathbb{Q}$, $p(x) = P_{\min}(a, \mathbb{Q}) = x - a$, $\deg p(x) = 1 = 2^0$

Supponiamo $t \geq 1$

$$\begin{cases} \mathbb{Q} = K_0 \preceq \dots \preceq K_t \\ [K_i : K_{i-1}] = 2 \quad \forall i = 1, \dots, t \end{cases} \xRightarrow{[2.19, \text{pg.17}]} [K_t : K_0] = 2^t$$

$$[K_t : K_0] \text{ finita} \Rightarrow [K_t : K_0] \text{ algebrica} \Rightarrow a \in K_t \text{ algebrico su } K_0 = \mathbb{Q} \Rightarrow \exists p(x) = P_{\min}(a, \mathbb{Q})$$

$$\begin{cases} \mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq K_t \\ [K_t : \mathbb{Q}] = 2^t \end{cases} \xRightarrow{[2.18, \text{pg.16}]} [\mathbb{Q}(a) : \mathbb{Q}] / 2^t \Rightarrow \exists m : [\mathbb{Q}(a) : \mathbb{Q}] = 2^m$$

$$\deg p(x) = [\mathbb{Q}(a) : \mathbb{Q}] = 2^m$$

□

Example 6.52.

1. E' impossibile rettificare la circonferenza
2. E' impossibile quadrare il cerchio
3. E' impossibile duplicare il cubo

Proof:

(1) Dim 1.

Rettificare una circonferenza di raggio r vuol dire costruire un segmento di lunghezza pari al perimetro della circonferenza, ovvero di lunghezza $2\pi r$, o in altri termini, deve essere $2\pi r \in \mathbb{E}$. Quindi,

$$\begin{aligned} 2\pi r \in \mathbb{E} &\xRightarrow{2, r \in \mathbb{E}, \mathbb{E} \text{ campo}} \pi \in \mathbb{E} \\ \pi \in \mathbb{E} &\xRightarrow{[6.51, \text{pg.131}]} \pi \text{ e' algebrico su } \mathbb{Q} \end{aligned}$$

e questo e' assurdo.

(2) Dim 2.

Quadrare il cerchio vuol dire costruire un quadrato di area pari all'area di un cerchio di raggio r . Quindi, dobbiamo trovare un $l \in \mathbb{E}$ tale che $l^2 = \pi r^2$.

$$l \in \mathbb{E} \Rightarrow l^2 \in \mathbb{E} \Leftrightarrow \pi r^2 \in \mathbb{E} \Rightarrow \pi \in \mathbb{E} \xRightarrow{[6.51, \text{pg.131}]} \pi \text{ e' algebrico su } \mathbb{Q}$$

Assurdo.

(3) Dim 3.

Dato un cubo di lato a e volume a^3 , bisogna trovare un cubo di volume $b^3 = 2a^3$, e quindi
 $b^3 = 2a^3 \Leftrightarrow b = \sqrt[3]{2a^3} = \sqrt[3]{2}a$

Se per assurdo $b \in \mathbb{E}$

$$b \in \mathbb{E} \Rightarrow \sqrt[3]{2}a \underbrace{\Rightarrow}_{a \in \mathbb{E}, \mathbb{E} \text{ campo}} \Rightarrow \sqrt[3]{2} \in \mathbb{E}$$

$$\sqrt[3]{2} \in \mathbb{E} \underbrace{\Rightarrow}_{[6.51, \text{pg.131}]} p(x) = P_{\min}(\sqrt[3]{2}, \mathbb{Q}) = 2^m$$

$$p(x) = P_{\min}(\sqrt[3]{2}, \mathbb{Q}) \underbrace{=}_{\text{vedi esercizio [8.3, pg.173]}} x^3 - 2 \Rightarrow \deg p(x) = 3$$

Assurdo.

□

6.3.1 Ciclotomia

Proposition 6.53. *E' possibile costruire un poligono regolare di n lati inscritto nella circonferenza unitaria $\Leftrightarrow \omega$ e' euclideo, dove $U_n = \langle \omega \rangle$.*

Proof: Sul piano complesso, le radici n -esime dell'unita' si dispongono proprio sui vertici del poligono regolare di n -lati, infatti,

$$\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

$$\omega^k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$$

(1) Dim $\Leftarrow$

Supponiamo che ω sia euclideo.

$$\omega \text{ euclideo} \Leftrightarrow \cos \frac{2\pi}{n}, \sin \frac{2\pi}{n} \in \mathbb{E} \underbrace{\Rightarrow}_{[6.49, \text{pg.127}]} P = \left(\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n} \right) \text{ e' un punto costruibile a partire da } A_0 = (0, 0)$$

Allora, anche il segmento PA_1 e' costruibile.

La radice $\omega^0 = 1 + i0 = 1$ corrisponde al punto $(1, 0) = A_1$.

La radice ω corrisponde al punto P .

Quindi il segmento PA_1 e' il primo lato del poligono.

Per costruire gli altri lati, basta usare il compasso:

$$c_1 = \mathcal{C}(P, \|\vec{PA_1}\|)$$

$$\{P_2, A_1\} = c_1 \cap S^1$$

S^1 e' la circonferenza unitaria

E' facile vedere che il secondo lato del poligono e' P_2P .

Procedendo in questo modo, si costruiscono tutti gli altri lati.

(2) $\Rightarrow$

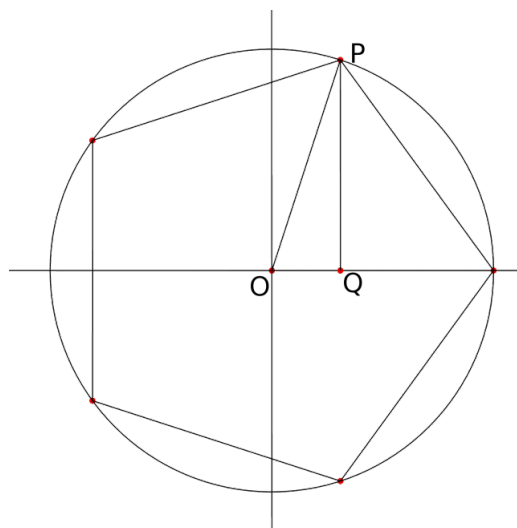
Per ipotesi possiamo costruire tutti i vertici del poligono regolare.

Possiamo anche supporre che $A_1 = (1, 0)$ sia un punto di tale poligono (se cosi' non fosse, base ricostruire gli assi).

Consideriamo un segmento che abbiamo per estremo A_1 e per altro estremo $P = (x, y)$, in modo che $y \geq 0$. Vedi figura per $n = 5$: E' facile vedere che

$$x = \cos \frac{2\pi}{n}$$

$$y = \sin \frac{2\pi}{n}$$



Quindi,

$$P = (x, y) \text{ costruibile} \quad \underbrace{\Rightarrow}_{[6.49, \text{pg.127}]} \quad x, y \in \mathbb{E} \Leftrightarrow x + iy \text{ e' euclideo}$$

□

Proposition 6.54. *Sia $U_n = \langle \omega \rangle$, allora*

$$\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \text{ e' euclideo} \Leftrightarrow \cos \frac{2\pi}{n} \in \mathbb{E}$$

Proof: $\Rightarrow$ si ha per definizione.

Per la $\Leftarrow$, basta osservare che una volta costruito il coseno e' possibile costruire il seno:

1. si costruisce la circonferenza unitaria, con gli assi X, Y
2. si riporta il coseno nel segmento OQ
3. si costruisce la perpendicolare a X passante per Q
4. si interseca tale retta con la circonferenza
5. l'ordinata del punto P di intersezione e' il seno cercato
6. si traccia la perpendicolare a Y per P , riportando cosi' l'ordinata di P in un segmento su Y

□

Theorem 6.55. *Sia $U_n = \langle \omega \rangle$, allora*

$$\omega \text{ e' euclideo} \Leftrightarrow \exists m \geq 0 : \varphi(n) = 2^m$$

dove φ e' la funzione di eulero.

Proof:

$$\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

Poniamo

$$\alpha = \cos \frac{2\pi}{n}, \quad \beta = \sin \frac{2\pi}{n}$$

(1) Dim. $\Rightarrow$

ω euclideo $\Leftrightarrow \alpha, \beta \in \mathbb{E}$

$$\alpha \in \mathbb{E} \quad \underbrace{\Rightarrow}_{[6.51, \text{pg.131}]} \deg P_{\min}(\alpha, \mathbb{Q}) = 2^m, \quad m \geq 0 \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m \quad (1)$$

$$\omega = \alpha + i\beta \in \mathbb{Q}(\alpha, \beta, i) \Rightarrow \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\alpha, \beta, i) \quad (1.1)$$

$$\alpha^2 + \beta^2 = \cos^2 \theta + \sin^2 \theta = 1 \Rightarrow \beta \text{ e' radice di } x^2 + \alpha^2 - 1 \in \mathbb{Q}(\alpha)[x] \quad (2)$$

$$(1.1) \quad \exists t \geq 0 : [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^t$$

Sia $p(x) = P_{\min}(\beta, \mathbb{Q}(\alpha))$. Partendo dalla (2), distinguiamo due casi:

CASE: $x^2 + \alpha^2 - 1$ riducibile in $\mathbb{Q}(\alpha)[x]$

$$x^2 + \alpha^2 - 1 = h(x)g(x), \quad \deg h(x) = \deg g(x) = 1, \quad h(x), g(x) \in \mathbb{Q}(\alpha)[x] \Rightarrow h(\beta) = 0 \vee g(\beta) = 0$$

$$\Rightarrow p(x) \mid h(x) \vee p(x) \mid g(x) \Rightarrow \deg p(x) = 1$$

$$\Rightarrow p(x) = x - \beta \in \mathbb{Q}(\alpha)[x] \Rightarrow \beta \in \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$$

$$\Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \underbrace{=}_{(1)} 2^m$$

CASE: $x^2 + \alpha^2 - 1$ irriducibile in $\mathbb{Q}(\alpha)[x]$

$$\begin{cases} x^2 + \alpha^2 - 1 \in \mathbb{Q}(\alpha)[x], \text{ irrid.} \\ \text{e' monico} \\ \beta \text{ e' una sua radice} \end{cases} \quad \underbrace{\Rightarrow}_{[2.30, \text{pg.24}]} \quad p(x) = x^2 + \alpha^2 - 1 \Rightarrow [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] = \deg p(x) = 2$$

$$\begin{cases} \mathbb{Q} \preceq \mathbb{Q}(\alpha) \preceq \mathbb{Q}(\alpha)(\beta) \\ [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] = 2 \\ [\mathbb{Q}(\alpha) : \mathbb{Q}] \underbrace{=}_{(1)} 2^m \end{cases} \quad \underbrace{\Rightarrow}_{[2.18, \text{pg.16}]} \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^{m+1}$$

$$(1.2) \quad \exists r > 0 : [\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^r$$

$$P_{\min}(i, \mathbb{Q}(\alpha, \beta)) = x^2 + 1 \Rightarrow [\mathbb{Q}(\alpha, \beta)(i) : \mathbb{Q}(\alpha, \beta)] = 2 \quad (3)$$

$$[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] \underbrace{=}_{[2.18, \text{pg.16}]} [\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}(\alpha, \beta)] [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \underbrace{=}_{(3), \text{ passo 1.1}} 2 \cdot 2^t = 2^{t+1}$$

In conclusione:

$$\begin{cases} \mathbb{Q} \preceq \mathbb{Q}(\omega) \preceq \mathbb{Q}(\alpha, \beta, i) \\ (1.1) \\ [\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^r \end{cases} \quad \underbrace{\Rightarrow}_{[2.18, \text{pg.16}]} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] / 2^r \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = 2^{r'} \quad \Leftrightarrow_{[6.42, \text{pg.114}]} \quad \varphi(n) = 2^{r'}$$

(1) Dim. $\Leftarrow$

Supponiamo $\varphi(n) = 2^m$.

$$\omega \text{ e' euclideo} \quad \Leftrightarrow_{[6.54, \text{pg.133}]} \quad \alpha \in \mathbb{E}$$

Per dimostrare $\alpha \in \mathbb{E}$ useremo il thm [6.50, pg.128].

Consideriamo l'operazione di coniugazione:

$$\sigma : \mathbb{C} \longrightarrow \mathbb{C}$$

$$z \mapsto \bar{z}$$

σ e' un omomorfismo di campi, infatti,

$$\overline{a+b} = \overline{a} + \overline{b}$$

$$\overline{ab} = \overline{a}\overline{b}$$

e' inoltre un isomorfismo (infatti $\sigma^{-1} = \sigma$). E' chiaro anche che $\sigma|_{\mathbb{R}} = \text{id}$.

Per il thm [6.42,pg.114] sappiamo:

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) \underbrace{=}_{\text{per Hp}} 2^m \quad (0)$$

$$\mathbb{Q} \preceq \mathbb{Q}(\omega) \text{ e' di Galois} \quad (1)$$

Allora

$$(1) \Rightarrow \mathbb{Q} \preceq \mathbb{Q}(\omega) \text{ algebrica} \quad \underbrace{\Rightarrow}_{[2.62, \text{pg.49}]} \quad \overline{\mathbb{Q}} = \overline{\mathbb{Q}(\omega)} \quad (1.1)$$

$$(1) \quad \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} \quad |\mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] \underbrace{=}_{(0)} 2^m \quad (1.2)$$

$$\begin{aligned}
& \text{Sia } \sigma' = \sigma|_{\mathbb{Q}(\omega)}. \\
& \sigma'(\omega) = \sigma'(\alpha + i\beta) = \alpha - i\beta \\
& \sigma'(\omega)\omega = (\alpha - i\beta)(\alpha + i\beta) = \alpha^2 + \beta^2 = \cos^2 \theta + \sin^2 \theta = 1 \Rightarrow \sigma'(\omega) = \omega^{-1} \\
& k = \deg P_{\min}(\omega, \mathbb{Q}) = [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) \\
& \omega \text{ algebrico} \Rightarrow \mathbb{Q}(\omega) = \{a_0 + a_1\omega + \dots + a_{k-1}\omega^{k-1} \mid a_i \in \mathbb{Q} \forall i = 0, \dots, k-1\} \\
& \sigma'(\underbrace{a_0 + a_1\omega + \dots + a_{k-1}\omega^{k-1}}_{\in \mathbb{Q}(\omega)}) \underbrace{=}_{\sigma' \text{ omo.}, \sigma'|_{\mathbb{R}} = \text{id}} a_0 + a_1\sigma'(\omega) + \dots + a_{k-1}\sigma'(\omega)^{k-1} = \\
& = a_0 + a_1\omega^{-1} + \dots + a_{k-1}(\omega^{-1})^{k-1} \in \mathbb{Q}(\omega^{-1}) \underbrace{\subseteq}_{\omega^{-1} \in \mathbb{Q}(\omega)} \mathbb{Q}(\omega)
\end{aligned}$$

$$\begin{aligned}
& \text{Quindi } \sigma'(\mathbb{Q}(\omega)) \subseteq \mathbb{Q}(\omega) \Leftrightarrow \text{Im } \sigma' \subseteq \mathbb{Q}(\omega) \\
& \left\{ \begin{array}{l} \sigma' : \mathbb{Q}(\omega) \longrightarrow \mathbb{Q}(\omega) \subseteq \overline{\mathbb{Q}(\omega)} = \overline{\mathbb{Q}} \\ \sigma \text{ omomorfismo} \Rightarrow \sigma' \text{ omomorfismo} \Rightarrow \\ \sigma|_{\mathbb{R}} = \text{id} \Rightarrow \sigma'|_{\mathbb{Q}} = \text{id} \end{array} \right. \Rightarrow \\
& \Rightarrow \sigma' \in \mathcal{I}(\mathbb{Q}(\omega), \mathbb{Q}) \underbrace{=}_{(1), [6.24, \text{pg.96}]} \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \Rightarrow H = \langle \sigma' \rangle \leq \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) = G \text{ sottogruppo}
\end{aligned}$$

$$\begin{aligned}
& \sigma'^{-1} = \sigma', \quad \sigma' \neq \text{id} \Rightarrow o(\sigma') = 2 \Rightarrow |H| = 2 \\
& \left\{ \begin{array}{l} \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \underbrace{\simeq}_{[6.43, \text{pg.118}]} U(\mathbb{Z}_n) \\ U(\mathbb{Z}_n) \text{ abeliano} \end{array} \right. \Rightarrow G = \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \text{ abeliano} \Rightarrow H \leq G \text{ e' normale}
\end{aligned}$$

$$\text{Nota che: } H \leq G \Rightarrow |G| \geq |H| = 2 \underbrace{\Rightarrow}_{|G|=2^m} m \geq 1$$

$$\begin{aligned}
& \left\{ \begin{array}{l} H \leq G = \mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \text{ normale} \\ (1) \end{array} \right. \underbrace{\Rightarrow}_{[6.31, \text{pg.105}]} \left\{ \begin{array}{l} \mathbb{Q} \preceq \mathbb{Q}(\omega)^H \text{ di Galois (4)} \\ [\mathbb{Q}(\omega)^H : \mathbb{Q}] = \frac{|G|}{|H|} \underbrace{=}_{(1.2)} \frac{2^m}{2} = 2^{m-1} \end{array} \right. \quad (4.1) \\
& (4) \Rightarrow |\mathcal{G}(\mathbb{Q}(\omega)^H, \mathbb{Q})| = [\mathbb{Q}(\omega)^H : \mathbb{Q}] \underbrace{=}_{(4.1)} 2^{m-1} \quad (4.2)
\end{aligned}$$

$$\text{Poniamo } \mathbb{H} = \mathbb{Q}(\omega)^H, \quad J = \mathcal{G}(\mathbb{H}, \mathbb{Q})$$

$$|J| \underbrace{=}_{(4.2)} 2^{m-1} \Rightarrow J \text{ e' un 2-gruppo} \Rightarrow$$

$$\begin{aligned}
& \underbrace{\Rightarrow}_{\text{thm } p\text{-gruppi [AII, 2.5, pg.80]}} \exists J_0 = \{\text{id}\} \leq J_1 \leq \dots \leq J_{m-1} = J \text{ tale che } \begin{cases} |J_i| = 2^i \\ J_i \leq J \text{ normale} \end{cases} \quad \forall i = 0, \dots, m-1 \quad (5) \\
& (1.1) \quad \mathbb{H} \subseteq \mathbb{R}
\end{aligned}$$

$$\begin{aligned}
& \mathbb{H} = \mathbb{Q}(\omega)^H = \mathbb{Q}(\omega)^{\{\text{id}, \sigma\}} = \{z \in \mathbb{Q}(\omega) \mid \sigma(z) = z \Leftrightarrow \bar{z} = z \Leftrightarrow z \in \mathbb{R}\} = \mathbb{Q}(\omega) \cap \mathbb{R} \\
& (1.2) \quad \mathbb{H}^J = \mathbb{Q}
\end{aligned}$$

$$\begin{aligned}
& \mathbb{H}^J = \mathbb{H}^{\mathcal{G}(\mathbb{H}, \mathbb{Q})} \underbrace{=}_{\text{corrispondenza Galois [6.25, pg.96]}} \mathbb{Q} \\
& (1.3) \quad \alpha \in \mathbb{H}
\end{aligned}$$

$$\frac{\omega + \sigma'(\omega)}{2} = \frac{\omega + \bar{\omega}}{2} = \cos \frac{2\pi}{n} = \alpha$$

$$\alpha = \frac{\omega + \bar{\omega}}{2} \in \mathbb{Q}(\omega)$$

$$\sigma'(\alpha) \underbrace{=}_{\sigma' \text{ omomorfismo}} \frac{\sigma'(\omega) + \sigma'\sigma'(\omega)}{\sigma'(2)} \underbrace{=}_{\sigma'|_{\mathbb{Q}(\omega)} = \text{id}} \frac{\sigma'(\omega) + \omega}{2} = \alpha$$

$$\sigma'(\alpha) = \alpha \in \mathbb{Q}(\omega) \Rightarrow \alpha \in \mathbb{Q}(\omega)^{\{\text{id}, \sigma'\}} = \mathbb{Q}(\omega)^H = \mathbb{H}$$

Usando la corrispondenza di Galois (vedi [6.25,pg.96]), dalla (5) abbiamo

$$\underbrace{\mathbb{Q} = \mathbb{H}^J}_{\text{passo 1.2}} = \mathbb{H}^{J_{m-1}} \preceq \mathbb{H}^{J_{m-2}} \preceq \dots \preceq \mathbb{H}^{J_1} \preceq \mathbb{H}^{J_0} = \mathbb{H}^{\{\text{id}\}} = \mathbb{H} \underbrace{\subseteq}_{\text{passo 1.1}} \mathbb{R} \quad (5.1)$$

$$(1.4) \quad [\mathbb{H}^{J_i} : \mathbb{H}^{J_{i+1}}] = 2 \quad \forall i = 0, \dots, m-2$$

$$[\mathbb{H} : \mathbb{Q}] = [\mathbb{Q}(\omega)^H : \mathbb{Q}] \underbrace{=}_{(4.2)} 2^{m-1}$$

$$\left\{ \begin{array}{l} (5) \Rightarrow J_i \leq J = \mathcal{G}(\mathbb{H}, \mathbb{Q}) \text{ normale} \\ \mathbb{Q} \preceq \mathbb{H} \text{ di Galois} \end{array} \right. \xRightarrow{[6.31, \text{pg.105}]} \left\{ \begin{array}{l} \mathbb{Q} \preceq \mathbb{H}^{J_i} \text{ e' di Galois (6.1)} \\ [\mathbb{H}^{J_i} : \mathbb{Q}] = \frac{|\mathcal{J}|}{|J_i|} \underbrace{=}_{(5)} \frac{2^{m-1}}{2^i} = 2^{m-1-i} \end{array} \right. \quad (6.2)$$

$$(5.1) \Rightarrow \left\{ \begin{array}{l} \mathbb{Q} \preceq \mathbb{H}^{J_i} \preceq \mathbb{H} \\ [\mathbb{H}^{J_i} : \mathbb{Q}] \underbrace{=}_{(6.2)} 2^{m-1-i} \\ [\mathbb{H} : \mathbb{Q}] \underbrace{=}_{(4.2)} 2^{m-1} \end{array} \right. \xRightarrow{[2.18, \text{pg.16}]} [\mathbb{H} : \mathbb{H}^{J_i}] = 2^i \quad (7)$$

$$\left\{ \begin{array}{l} \mathbb{H}^{J_{i+1}} \subseteq \mathbb{H}^{J_i} \subseteq \mathbb{H} \\ [\mathbb{H} : \mathbb{H}^{J_i}] \underbrace{=}_{(7)} 2^i \\ [\mathbb{H} : \mathbb{H}^{J_{i+1}}] \underbrace{=}_{(7)} 2^{i+1} \end{array} \right. \xRightarrow{[2.18, \text{pg.16}]} [\mathbb{H}^{J_i} : \mathbb{H}^{J_{i+1}}] = \frac{2^{i+1}}{2} = 2$$

(1.5) Q.E.D.

$$\left\{ \begin{array}{l} \alpha \underbrace{\in}_{\text{passo 1.3}} \mathbb{H} \\ (5.1) \Rightarrow \mathbb{Q} = \mathbb{H}^{J_{m-1}} \preceq \mathbb{H}^{J_{m-2}} \preceq \dots \preceq \mathbb{H}^{J_1} \preceq \mathbb{H}^{J_0} = \mathbb{H} \subseteq \mathbb{R} \\ m \geq 1 \\ [\mathbb{H}^{J_i} : \mathbb{H}^{J_{i+1}}] = 2 \quad \forall i = 0, \dots, m-2 \end{array} \right. \xRightarrow{[6.50, \text{pg.128}]} \alpha \in \mathbb{E}$$

che e' la tesi. □

Proposition 6.56. Sia $n = 2^{s_0} p_1^{s_1} \dots p_t^{s_t}$ la fattorizzazione in primi distinti di n , con $s_0 \geq 0$,

$s_i > 0 \quad \forall i = 1, \dots, t$, allora

$$\begin{aligned}\varphi(n) = 2^m &\Leftrightarrow \begin{cases} s_1 = s_2 = \dots = s_t = 1 \\ p_i = 2^{2^{h_i}} + 1 \quad \forall i = 1 \dots t \end{cases} \\ \varphi(n) = 2^m &\Rightarrow n = 2^{s_0} (2^{2^{h_1}} + 1) \dots (2^{2^{h_t}} + 1) \\ &\text{con } k_i, h_i \geq 0\end{aligned}$$

Proof: Supporremo $s_0 > 0$. La dimostrazione e' analoga nel caso $s_0 = 0$ (basta non considerare 2^{s_0}).

Per la prop [AI,12.3,pg.55], abbiamo

$$\begin{aligned}\varphi(n) &= n \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right) = \\ &= 2^{s_0} \left(1 - \frac{1}{2}\right) p_1^{s_1} \left(1 - \frac{1}{p_1}\right) \dots p_t^{s_t} \left(1 - \frac{1}{p_t}\right) = 2^{s_0-1} p_1^{s_1-1} (p_1 - 1) \dots p_t^{s_t-1} (p_t - 1) \\ \varphi(n) = 2^m &\Leftrightarrow \begin{cases} s_1 = s_2 = \dots = s_t = 1 \\ p_i - 1 = 2^{r_i} \quad \forall i = 1, \dots, t \end{cases} \quad (1)\end{aligned}$$

(1) Dimostriamo che

$$2^r + 1 \text{ primo} \Rightarrow r = 0 \vee \exists h \geq 0 : r = 2^h$$

(Non vale il viceversa: $2^{32} + 1$ non e' primo)

Se $r = 0$ allora la tesi e' vera. Supponiamo $r \neq 0$.

Supponiamo per assurdo che r non sia una potenza di 2, ovvero

$$r = 2^k d \quad \text{con } d \text{ dispari, } d \neq 1$$

allora

$$2^r + 1 = 2^{2^k d} + 1 = \left(2^{2^k}\right)^d + 1 \quad (*)$$

Il polinomio $x^d + 1$ ammette -1 come radice (d e' dispari), quindi applicando Ruffini otteniamo:

$$x^d + 1 = (x + 1)(1 - x + x^2 - x^3 + \dots + x^{d-3} - x^{d-2} + x^{d-1})$$

quindi, la (*) diventa:

$$x = 2^{2^k}$$

$$2^r + 1 = 2^{2^k d} + 1 = x^d + 1 = (x + 1)(1 - x + x^2 - x^3 + \dots + x^{d-3} - x^{d-2} + x^{d-1})$$

Ma $2^r + 1$ e' primo, quindi

$$x + 1 = \pm 1 \quad \vee \quad 1 - x + x^2 - x^3 + \dots + x^{d-3} - x^{d-2} + x^{d-1} = \pm 1$$

Analizziamo i vari casi:

$$x + 1 = -1 \Leftrightarrow x = -2 \text{ assurdo perche' } x = 2^{2^k} > 0$$

$$x + 1 = 1 \Leftrightarrow x = 0 \text{ assurdo}$$

$$\begin{cases} x + 1 > 0 \\ x^d + 1 > 0 \end{cases} \Rightarrow 1 - x + x^2 - x^3 + \dots + x^{d-3} - x^{d-2} + x^{d-1} = -1 > 0 \quad \text{assurdo}$$

Quindi l'unico caso rimasto e':

$$-x + x^2 - x^3 + \dots + x^{d-3} - x^{d-2} + x^{d-1} = 0 \Leftrightarrow_{x \neq 0} -1 + x - x^2 + \dots + x^{d-4} - x^{d-3} + x^{d-2} = 0 \Rightarrow$$

$$\Rightarrow -1 = 0 \quad \mathbb{Z}_x \Leftrightarrow x/1 \Leftrightarrow 2^{2^k}/1 \Rightarrow 2^{2^k} = 1 \text{ assurdo}$$

Quindi

$$p_i - 1 = 2^{r_i} \Leftrightarrow p_i = 2^{r_i} + 1 \quad \underbrace{\Rightarrow}_{p_i \text{ primo, passo 1}} \quad r_i = 0 \vee r_i = 2^{h_i} \Leftrightarrow p_i = 2 \vee p_i = 2^{2^{h_i}} + 1 \quad \underbrace{\Leftrightarrow}_{\text{Per Hp } p_i \neq 2} \quad p_i = 2^{2^{h_i}} + 1 \quad (2)$$

In conclusione, dalla (1) e (2) abbiamo

$$\varphi(n) = 2^m \Leftrightarrow \begin{cases} s_1 = s_2 = \dots = s_t = 1 \\ p_i = 2^{2^{h_i}} + 1 \quad \forall i = 1, \dots, t \end{cases} \Rightarrow n = 2^{s_0} p_1^{s_1} \dots p_t^{s_t} = 2^{s_0} (2^{2^{h_1}} + 1) \dots (2^{2^{h_t}} + 1)$$

□

Proposition 6.57. *Sia dato il seguente algoritmo scritto in J²³*

`rc=:3 : '-. (+./ 1 >~ #/.~ ([ #~ 2&|) q: y) +. (-.*./ 1=+/"1#: ~.1-~q: y)' "0`

allora

$$rc\ n = 1 \Leftrightarrow \varphi(n) = 2^m$$

7 Gruppi risolubili

Definition 7.1. Sia G un gruppo

G e' un gruppo risolubile $\Leftrightarrow$

$$\Leftrightarrow \exists \text{catena di gruppi } \{e\} = H_0 \leq H_1 \leq \dots \leq H_n = G \text{ t.c. } \begin{cases} H_{i-1} \leq H_i \text{ normale} \\ \frac{H_i}{H_{i-1}} \text{ e' abeliano} \end{cases} \quad \forall i = 1, \dots, n$$

La catena viene chiamata *catena risolvibile*.

Proposition 7.2.

1. G abeliano $\Rightarrow G$ risolubile
2. G p -gruppo $\Rightarrow G$ risolubile
3. $|G| = pq$, p, q primi $\Rightarrow G$ risolubile

Proof:

(1) Dim 1.

Basta scegliere la catena banale $H_0 = \{e\} \leq H_1 = G$.

(2) Dim 2.

$$G \text{ } p\text{-gruppo} \xRightarrow{\text{thm } p\text{-gruppi [AII,2.5,pg.80]}} \exists H_0 = \{id\} \leq H_1 \leq \dots \leq H_k = G \text{ tale che } \begin{cases} |H_i| = p^i \\ H_i \leq G \text{ normale} \end{cases} \quad \forall i = 0, \dots, k$$

$$H_{i-1} \leq G \text{ normale} \xRightarrow{H_i \subseteq G} H_{i-1} \leq H_i \text{ normale}$$

$$\left| \frac{H_i}{H_{i-1}} \right| \xRightarrow{[AII,1.114,pg.47]} \frac{|H_i|}{|H_{i-1}|} = \frac{p^i}{p^{i-1}} = p \text{ primo} \xRightarrow{[AII,1.56,pg.20]} \frac{H_i}{H_{i-1}} \text{ ciclico} \Rightarrow \frac{H_i}{H_{i-1}} \text{ abeliano}$$

(3) Dim 3.

Distinguiamo due casi

CASE: $p = q$

$$|G| = pq \xRightarrow{p=q} p^2 \xRightarrow{[AII,2.6,pg.81]} G \text{ e' abeliano} \xRightarrow{1.} G \text{ e' risolubile}$$

²³Vedi Jsoftware <http://www.jsoftware.com/>

CASE: $p \neq q$

Possiamo supporre $q > p$. Applichiamo il thm di Cauchy e di Sylow

$$\begin{cases} |G| = pq \\ p \neq q \end{cases} \xRightarrow{\text{Sylow [AII,2.8,pg.83]}} \exists K \leq G : |K| = q$$

Sia t il numero di q sottogruppi di Sylow, sempre per il thm [AII,2.8,pg.83] si ha

$$\begin{cases} t/p \\ t = 1 \pmod{q} \end{cases} \xRightarrow{q > p} t = 1$$

quindi esiste un unico q -sottogruppo di Sylow, cioè K .

Allora, per la prop [AII,2.9,pg.88] si ha che K è normale in G .

Infine,

$$\begin{cases} G \text{ finito} \\ K \text{ normale in } G \end{cases} \xRightarrow{\text{[AII,1.114,pg.47]}} \left| \frac{G}{K} \right| = \frac{|G|}{|K|} = \frac{pq}{q} = p \text{ primo} \xRightarrow{\text{[AII,1.56,pg.20]}} \frac{G}{K} \text{ ciclico} \Rightarrow \frac{G}{K} \text{ abeliano}$$

$$|K| = q \text{ primo} \Rightarrow K \text{ ciclico, e quindi abeliano} \Rightarrow K \simeq \frac{K}{\{e\}} \text{ abeliano}$$

Quindi come catena possiamo scegliere

$$\{e\} \leq K \leq G$$

□

Proposition 7.3. *Sia dato un gruppo G risolubile, allora*

1. $H \leq G \Rightarrow H$ risolubile

2. $N \leq G$ normale $\Rightarrow \frac{G}{N}$ risolubile

3. $1 < |G| < +\infty \Rightarrow \exists$ una catena risolvibile $\{e\} = H_0 \leq \dots \leq H_n = G$ t.c. $\left| \frac{H_i}{H_{i-1}} \right| = p_i$ primo $\forall i = 1, \dots, n$

Proof:

$$G \text{ risolubile} \Rightarrow \exists \{e\} = K_0 \leq K_1 \leq \dots \leq K_n = G \text{ t.c. } \begin{cases} K_{i-1} \leq K_i \text{ normale} \\ \frac{K_i}{K_{i-1}} \text{ e' abeliano} \end{cases} \quad \forall i = 1, \dots, n \quad (1)$$

(1) Dim 1.

Consideriamo la catena di gruppi

$$H \cap \{e\} = \{e\} \leq H \cap K_1 \leq \dots \leq H \cap K_n = H \cap G = H$$

dimostriamo che è la catena risolvibile di H .

$$K_{i-1} \leq K_i \text{ normale} \xRightarrow{\text{[AII,1.181,pg.78]}} H \cap K_{i-1} \leq H \cap K_i \text{ normale}$$

Consideriamo il seguente omomorfismo:

$$K_i \cap H \xrightarrow{\text{id}} K_i \xrightarrow{\pi} \frac{K_i}{K_{i-1}}$$

$\varphi = \pi \circ \text{id}$, dove π è la suriezione naturale

$$\varphi(k) = kK_{i-1}$$

si ha

$$\ker \varphi = \{k \in K_i \cap H \mid kK_{i-1} = K_{i-1} \Leftrightarrow k \in K_{i-1}\} = K_i \cap H \cap K_{i-1} \underset{K_{i-1} \subseteq K_i}{=} H \cap K_{i-1}$$

$$\varphi \text{ omomorf.} \quad \Rightarrow \quad \frac{K_i \cap H}{\ker \varphi} = \frac{K_i \cap H}{H \cap K_{i-1}} \simeq \text{Im } \varphi \leq \frac{K_i}{K_{i-1}}$$

[AII,1.147,pg.60]

$$\begin{cases} \frac{H \cap K_i}{H \cap K_{i-1}} \leq \frac{K_i}{K_{i-1}} \\ \frac{K_i}{K_{i-1}} \text{ abeliano} \end{cases} \Rightarrow \frac{H \cap K_i}{H \cap K_{i-1}} \text{ abeliano}$$

(2) Dim 2.

$$\begin{cases} N \leq G \text{ normale} \\ K_i \leq G \end{cases} \Rightarrow NK_i \leq G$$

[AII,1.119,pg.49]

Possiamo così considerare la catena:

$$N \{e\} = N \leq NK_1 \leq \dots \leq NK_n = NG = G$$

$$\begin{cases} N \subseteq NK_i \subseteq G \\ N \leq G \text{ normale} \end{cases} \Rightarrow N \leq NK_i \text{ normale}$$

Applicando alla catena la suriezione naturale $\pi : G \longrightarrow \frac{G}{N}$, otteniamo:

$$\frac{N}{N} = \{N\} \leq \frac{NK_1}{N} \leq \dots \leq \frac{G}{N}$$

Dimostriamo che questa è la catena risolvibile cercata.

(2.1) Dim che $\frac{NK_{i-1}}{N} \leq \frac{NK_i}{N}$ è normale

Applicando il teorema di corrispondenza di gruppi (vedi [AII,1.158,pg.66]) alla suriezione naturale

$$\pi_i : NK_i \longrightarrow \frac{NK_i}{N} \text{ suriez. naturale}$$

abbiamo

$$H \leq NK_i \text{ normale t.c. } H \supseteq \ker \pi_i \quad \Leftrightarrow \quad \pi_i(H) \leq \pi_i(NK_i) \text{ normale} \Leftrightarrow \frac{H}{N} \leq \frac{NK_i}{N} \quad (2)$$

[AII,1.158,pg.66]

In particolare,

$$\ker \pi_i = N \subseteq NK_{i-1}$$

$$NK_{i-1} \leq NK_i \text{ normale} \quad \Leftrightarrow \quad \frac{NK_{i-1}}{N} \leq \frac{NK_i}{N} \text{ normale}$$

(2)

(2.1.1) Dim. che $NK_{i-1} \leq NK_i$ normale

Usiamo la caratterizzazione dei sott. normali (vedi [AII,1.104,pg.42])

Siano $n_i k_i \in NK_i$, $n_{i-1} k_{i-1} \in NK_{i-1}$

$$(n_i k_i)(n_{i-1} k_{i-1})(n_i k_i)^{-1} = n_i k_i n_{i-1} k_{i-1} k_i^{-1} n^{-1}_i =$$

$$N \leq G \text{ normale} \Rightarrow k_i N = N k_i \Rightarrow k_i n_{i-1} = n'_i k_i$$

$$= n_i n'_i k_i k_{i-1} k_i^{-1} n^{-1}_i =$$

$$K_{i-1} \leq K_i \text{ normale} \Rightarrow k_i k_{i-1} k_i^{-1} = k'_{i-1} \in K_{i-1}$$

$$= n_i n'_i k'_{i-1} n^{-1}_i =$$

$$N \leq G \text{ normale} \Rightarrow k'_{i-1} n^{-1}_i = n'_i k'_{i-1}$$

$$= n_i n'_i n'_i k'_{i-1} \in NK_{i-1}$$

$$\text{Quindi } \forall b \in NK_{i-1} \forall a \in NK_i \quad aba^{-1} \in NK_{i-1}$$

⟨2.2⟩ Dim che

$$\frac{\frac{NK_i}{N}}{\frac{NK_{i-1}}{N}}$$

e' abeliano

$$\left\{ \begin{array}{l} N \leq G \text{ normale} \Rightarrow N \leq NK_i \text{ normale} \\ NK_{i-1} \leq NK_i \text{ normale} \\ N \subseteq NK_{i-1} \end{array} \right. \xRightarrow{[\text{AII}, 1.155, \text{pg.64}]} \frac{\frac{NK_i}{N}}{\frac{NK_{i-1}}{N}} \simeq \frac{NK_i}{NK_{i-1}} \xRightarrow{[\text{AII}, 1.118, \text{pg.48}]} \frac{K_i N}{K_{i-1} N}$$

Allora, basta dimostrare che $K_i N / K_{i-1} N$ e' abeliano.

Consideriamo il seguente omomorfismo:

$$K_i \xrightarrow{\text{id}} K_i N \xrightarrow{\pi} \frac{K_i N}{K_{i-1} N}$$

$\varphi = \pi \circ \text{id}$, dove π e' la suriezione naturale

$$\varphi(k_i) = k_i K_{i-1} N$$

φ e' surriettiva, infatti,

$$k_i n K_{i-1} N \xrightarrow{N \subseteq K_{i-1} N} k_i K_{i-1} N = \varphi(k_i)$$

quindi per il thm dell'omomorfismo ([AII, 1.147, pg.60]) abbiamo l'isomorfismo $\bar{\varphi}$,

$$\frac{K_i}{\ker \varphi} \xrightarrow{\bar{\varphi}} \text{Im } \varphi = \frac{K_i N}{K_{i-1} N}$$

inoltre

$$\ker \varphi = K_i \cap K_{i-1} N \supseteq K_{i-1}$$

$$K_{i-1} \leq K_i \text{ normale} \Rightarrow \frac{K_i}{K_{i-1}} \text{ gruppo}$$

Sia

$$\psi : \frac{K_i}{K_{i-1}} \longrightarrow \frac{K_i}{\ker \varphi}$$

$$\psi(k_i K_{i-1}) = k_i \ker \varphi$$

⟨2.2.1⟩ ψ e' ben posta ed e' un omomorfismo

$$\text{Sia } k_i K_{i-1} = k'_i K_{i-1} \Leftrightarrow k_i = k'_i k_{i-1}$$

$$\psi(k_i K_{i-1}) = k_i \ker \varphi = k'_i k_{i-1} \ker \varphi \xrightarrow{K_{i-1} \subseteq \ker \varphi} k'_i \ker \varphi = \psi(k'_i K_{i-1})$$

quindi e' ben posta.

$$\psi(k_i K_{i-1}) \psi(k'_i K_{i-1}) = k_i \ker \varphi k'_i \ker \varphi = k_i k'_i \ker \varphi = \psi(k_i k'_i K_{i-1})$$

quindi e' un omomorfismo.

ψ e' chiaramente surriettiva.

Sia

$$\psi' : \frac{K_i}{K_{i-1}} \longrightarrow \frac{K_i N}{K_{i-1} N}$$

$$\psi' = \bar{\varphi} \circ \psi$$

$$\bar{\varphi}, \psi \text{ omo. surriettivi} \Rightarrow \psi' \text{ omo. surriettivo}$$

Possiamo adesso dimostrare l'abelianita' di $\frac{K_i N}{K_{i-1} N}$:

$$a', b' \in \frac{K_i N}{K_{i-1} N} \xRightarrow[\psi' \text{ surr.}]{\exists a, b \in \frac{K_i}{K_{i-1}} : \psi'(a) = a', \psi'(b) = b'}$$

$$a, b \in \frac{K_i}{K_{i-1}} \text{ abeliano} \Rightarrow ab = ba$$

$$a'b' = \psi'(a)\psi'(b) = \psi'(ab) = \psi'(ba) = \psi'(b)\psi'(a) = b'a'$$

(3) Dim. 3.

Procediamo per induzione forte su $|G| = m'$.

(3.1) $|G| = 2$

$$|G| = 2 \Rightarrow G \text{ abeliano}$$

La catena cercata e':

$$\{\mathbf{e}\} \leq G$$

(3.2) $|G| = m < m'$

Sia

$$\{\mathbf{e}\} = K_0 \leq \dots \leq K_n = G$$

la catena risolvete di G . Poiche' $|G| > 1 \Rightarrow G \neq \{\mathbf{e}\}$, possiamo supporre che gli elementi della catena siano distinti tra loro, ovvero

$$K_i \neq K_j \quad \forall i \neq j \quad (3)$$

(togliendo gli elementi non distinti da una catena risolvete otteniamo ancora una catena risolvete). Quindi,

$$\begin{cases} K_{n-1} \leq K_n \text{ normale} \\ |K_n| = |G| < \infty \end{cases} \xRightarrow{[AII, 1.114, \text{pg.47}]} \left| \frac{K_n}{K_{n-1}} \right| = \frac{|K_n|}{|K_{n-1}|}$$

$$\begin{cases} K_{n-1} \leq K_n \\ K_{n-1} \neq K_n \end{cases} \Rightarrow |K_{n-1}| < |K_n| \Rightarrow l = \frac{|K_n|}{|K_{n-1}|} > 1 \Rightarrow \exists p \text{ primo t.c. } p \nmid \left| \frac{K_n}{K_{n-1}} \right| \quad (*)$$

$$\text{Sia } G' = \frac{K_n}{K_{n-1}}, \quad d = \frac{|G'|}{p}$$

$$\begin{cases} G' \text{ abeliano} \\ d \nmid |G'| \end{cases} \xRightarrow{[AII, 3.4, \text{pg.93}]} \exists H' \leq G' \text{ t.c. } |H'| = d$$

$$\begin{cases} H' \leq G' \\ G' \text{ abeliano} \end{cases} \Rightarrow H' \leq G' \text{ normale} \quad (4)$$

Sia

$$\pi : K_n \longrightarrow \frac{K_n}{K_{n-1}} \text{ surriez. naturale}$$

$$H = \pi^{-1}(H')$$

Per il thm di corrispondenza (vedi [AII, 1.158, pg.66]) applicato a π , abbiamo

$$(4) \Leftrightarrow H' \leq G' \text{ normale} \xLeftrightarrow{[AII, 1.158, \text{pg.66}]} H = \pi^{-1}(H') \leq G \text{ normale t.c. } H \supseteq \ker \pi = K_{n-1}$$

Osserviamo che

$$\begin{aligned}
H' = \pi(H) &\Rightarrow H' = \frac{H}{K_{n-1}} \\
\left\{ \begin{array}{l} H \supseteq K_{n-1} \\ H, K_{n-1} \leq G \text{ normale} \end{array} \right. &\xRightarrow{[\text{AII}, 1.155, \text{pg. } 64]} \frac{\frac{K_n}{K_{n-1}}}{\frac{H}{K_{n-1}}} \simeq \frac{K_n}{H} \\
\frac{G'}{H'} = \frac{\frac{K_n}{K_{n-1}}}{\frac{H}{K_{n-1}}} &\xRightarrow{[\text{AII}, 1.155, \text{pg. } 64]} \frac{K_n}{H} \\
&\Rightarrow \left| \frac{K_n}{H} \right| = \left| \frac{G'}{H'} \right| = \frac{|G'|}{|H'|} = \frac{|G'|}{d} = p \\
\left| \frac{K_n}{H} \right| = p \text{ primo} &\Rightarrow \frac{K_n}{H} \text{ abeliano}
\end{aligned}$$

Abbiamo così dimostrato che

$$H \leq K_n = G \text{ normale}, \quad \left| \frac{G}{H} \right| = p \text{ primo}, \quad \frac{G}{H} \text{ abeliano}$$

Infine,

$$\left\{ \begin{array}{l} H \leq G \\ G \text{ risolubile} \end{array} \right. \xRightarrow{1.} H \text{ risolubile}$$

Possiamo allora applicare l'Hp induttiva su H , ottenendo la catena cercata:

$$\{\mathbf{e}\} = H_0 \leq H_1 \leq \dots \leq H_{n'-1} \leq H \leq G$$

□

Proposition 7.4. *Sia G un gruppo, allora*

$$\left\{ \begin{array}{l} N \leq G \text{ normale} \\ N \text{ risolubile} \\ \frac{G}{N} \text{ risolubile} \end{array} \right. \Rightarrow G \text{ risolubile}$$

Proof: N e $\frac{G}{N}$ sono risolubili, quindi abbiamo due catene risolventi:

$$\{\mathbf{e}\} = N_0 \leq \dots \leq N_n = N$$

$$\{\mathbf{e}'\} = H_0 \leq \dots \leq H_m = \frac{G}{N}$$

Sia

$$\pi : G \longrightarrow \frac{G}{N} \text{ surriez. naturale}$$

$$K_i = \pi^{-1}(H_i)$$

Per il thm di corrispondenza (vedi [AII, 1.157, pg. 65]):

$$H_i \leq \frac{G}{N} \Leftrightarrow K_i = \pi^{-1}(H_i) \leq G \text{ t.c. } K_i \supseteq \ker \pi = N \quad (5)$$

$$K_0 = \pi^{-1}(H_0) = \pi^{-1}(\{\mathbf{e}'\}) = N$$

$$K_m = \pi^{-1}(H_m) = \pi^{-1}\left(\frac{G}{N}\right) = G$$

abbiamo allora la catena:

$$\{\mathbf{e}\} = N_0 \leq \dots \leq N_n = N = K_0 \leq K_1 \leq \dots \leq K_m = G$$

Il primo pezzo della catena ($N_0 \leq \dots \leq N$) rispetta, per Hp, le proprietà di una catena

risolvente. Controlliamo che pure il secondo pezzo sia risolvente:

$$H_i = \pi(K_i) = \frac{K_i}{N} \quad (6)$$

$$\begin{cases} N \leq G \text{ normale} \\ N \subseteq K_i \subseteq G \end{cases} \Rightarrow N \leq K_i \text{ normale} \Rightarrow \frac{K_i}{N} \text{ gruppo}$$

$$\text{Sia } \pi_i = \pi|_{K_i} : K_i \longrightarrow \underbrace{\frac{K_i}{N}}_{(6)} = H_i \text{ surriez. naturale}$$

$$H_0 \leq \dots \leq H_m \text{ risolvente} \Rightarrow H_{i-1} \leq H_i \text{ normale} \quad \Leftrightarrow \quad K_{i-1} = \pi_i^{-1}(H_{i-1}) \leq K_i \text{ normale}$$

thm corrispondenza [AII, 1.158, pg. 66]

Verifichiamo l'abelianita':

$$\begin{aligned} \frac{H_i}{H_{i-1}} &\underbrace{=}_{(6)} \frac{\frac{K_i}{N}}{\frac{K_{i-1}}{N}} \underbrace{\simeq}_{[AII, 1.155, \text{pg. } 64]} \frac{K_i}{K_{i-1}} \\ H_0 \leq \dots \leq H_m \text{ risolvente} &\Rightarrow \frac{H_i}{H_{i-1}} \simeq \frac{K_i}{K_{i-1}} \text{ abeliano} \end{aligned}$$

□

Theorem 7.5. di Feit-Thompson.

Sia G un gruppo, allora

$$|G| \text{ dispari} \Rightarrow G \text{ risolubile}$$

Proof: Alcuni commenti riguardanti la dimostrazione:

It takes a professional group theorist about a year of hard work to understand the proof completely²⁴

La dimostrazione originale occupava un intero numero della rivista *Pacific Journal of Mathematics*: FEIT, W. AND THOMPSON, J. G. 1963. Solvability of groups of odd order. *Pacific J. Math.* 13:775-1029. (vedi²⁵)

L'intero numero di Pacific J. si puo' scaricare da qui:

<http://projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.pjm/1103053941>

□

7.1 Risolubilita' di S_n

Proposition 7.6. S_n e' risolubile $\forall n = 1, \dots, 4$

Proof:

(1) $n = 1, 2$

S_1, S_2 sono abeliani e quindi risolubili.

(2) $n = 3$

Una catena risolvente e'

$$\{\text{id}\} \leq A_3 \leq S_3$$

²⁴http://en.wikipedia.org/wiki/Feit-Thompson_theorem

²⁵Paragrafo *Solvable groups* nel capitolo *Subnormal Series; Solvable and Nilpotent Groups* di <http://www.jmilne.org/math/CourseNotes/math594g.html>

Infatti,

$$|A_3| = \frac{|S_3|}{2} = \frac{6}{2} = 3 \text{ primo} \Rightarrow A_3 \text{ ciclico} \Rightarrow A_3 \simeq \frac{A_3}{\{\text{id}\}} \text{ abeliano}$$

$$|A_3| = \frac{|S_3|}{2} \Rightarrow A_3 \leq S_3 \text{ e' normale}$$

$$\left| \frac{S_3}{A_3} \right| = 2 \Rightarrow \frac{S_3}{A_3} \text{ ciclico e quindi abeliano}$$

(3) $n = 4$

Una catena risolvibile e'

$$\{\text{id}\} \leq V \leq A_4 \leq S_4$$

dove V e' il gruppo Vier:

$$V = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

$$|A_4| = \frac{S_4}{2} \Rightarrow A_4 \leq S_4 \text{ normale}$$

$$\frac{S_4}{A_4} \text{ ha ordine 2 e quindi e' abeliano}$$

$$V \leq A_4 \text{ e' normale (vedi [AII,1.88,pg.34])}$$

$$\left| \frac{A_4}{V} \right| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3 \text{ primo} \Rightarrow \frac{A_4}{V} \text{ abeliano}$$

$$\frac{V}{\{\text{e}\}} \simeq V \text{ e' abeliano (vedi [AII,1.88,pg.34])}$$

□

Theorem 7.7. S_n non e' risolubile $\forall n \geq 5$

Proof:

(1) A_n non e' risolubile

Poiche', per $n \geq 5$, A_n e' semplice (non ha sottogruppi normali non banali, vedi [AII,1.91,pg.36]), l'unica possibile catena risolubile e'

$$\{\text{e}\} \subseteq A_n$$

Pero', A_n non e' abeliano, infatti, se lo fosse ogni suo sottogruppo dovrebbe essere normale.

A_n non risolubile

$$\Rightarrow$$

$\Rightarrow S_n$ non e' risolubile

sott. di un gruppo risolubile e' risolubile [7.3,pg.140]

□

7.2 Estensioni risolubili

Definition 7.8. Sia $F \preceq K$ una estensione algebrica. Definiamo la *traccia* e *norma*.

$$\text{Tr}_{K,F} : K \longrightarrow \overline{F}$$

$$\text{Tr}_{K,F}(\alpha) = \sum_{\sigma \in \mathcal{I}(K,F)} \sigma(\alpha)$$

$$\mathcal{N}_{K,F} : K \longrightarrow \overline{F}$$

$$\mathcal{N}_{K,F}(\alpha) = \prod_{\sigma \in \mathcal{I}(K,F)} \sigma(\alpha)$$

Proposition 7.9.

$$F \preceq K \text{ e' di Galois} \Rightarrow \text{Tr}_{K,F}(\alpha), \mathcal{N}_{K,F}(\alpha) \in F$$

Proof:

$$F \preceq K \text{ Galois} \xRightarrow{\substack{[6.19, \text{pg.} 92]}} F = K^{\mathcal{G}(K,F)} \quad (1)$$

$$F \preceq K \text{ Galois} \xRightarrow{\substack{[6.24, \text{pg.} 96]}} \mathcal{I}(K, F) = \mathcal{G}(K, F) \quad (2)$$

Sia $\sigma \in \mathcal{I}(K, F)$, si ha

$$\text{Tr}(\alpha) = \sum_{s \in \mathcal{I}(K,F)} s(\alpha) = \sum_{s \in \mathcal{G}(K,F)} s(\alpha) \xRightarrow{\substack{s: K \rightarrow K}} K \quad (2.1)$$

$$\sigma \in \mathcal{G}(K, F) \Rightarrow \sigma : K \rightarrow K$$

Possiamo allora considerare $\sigma(\text{Tr}(\alpha))$

$$\sigma(\text{Tr}(\alpha)) \xRightarrow{\substack{\sigma \text{ omomo. } s \in \mathcal{G}(K,F)}} \sum \sigma s(\alpha) \quad (3)$$

Sia $G = \mathcal{G}(K, F)$, per il lemma [AII, 1.52, pg. 19] si ha

$$G \leftrightarrow \sigma G = \{\sigma g \mid g \in G\}$$

quindi la (3) diventa

$$\begin{aligned} \sigma(\text{Tr}(\alpha)) &= \sum_{s \in \mathcal{G}(K,F)} \sigma s(\alpha) = \sum_{s \in \mathcal{G}(K,F)} s(\alpha) = \text{Tr}(\alpha) \\ &\Rightarrow \sigma(\text{Tr}(\alpha)) = \text{Tr}(\alpha) \end{aligned}$$

$$\text{Per l'arbitrarieta' di } \sigma \text{ e per la (2.1) si ha quindi } \text{Tr}(\alpha) \in K^{\mathcal{G}(K,F)} \xRightarrow{(1)} F$$

Analogamente si dimostra che $\mathcal{N}(\alpha) \in F$ □

Definition 7.10. Sia $F \preceq K$ una estensione finita e separabile. Sia $B = \{a_1, \dots, a_n\}$ una base dello spazio vettoriale K_F , con $n = \dim K_F = [K : F]$. Per il cor [6.10, pg. 84] possiamo così enumerare gli elementi di $\mathcal{I}(K, F)$:

$$\mathcal{I}(K, F) = \{\sigma_1, \dots, \sigma_n\}, \quad \text{con } \sigma_1, \dots, \sigma_n \text{ distinti fra loro}$$

Sia definita la seguente matrice

$$\begin{aligned} A &\in \overline{F}^{n \times n} \\ A_{ij} &= \sigma_i(a_j) \end{aligned}$$

Definiamo il *discriminante*:

$$\Delta \stackrel{\text{def}}{=} \det A$$

Proposition 7.11. Nelle ipotesi di [7.10, pg. 147] e definita la seguente matrice

$$\begin{aligned} T &\in \overline{F}^{n \times n} \\ T_{ij} &= \text{Tr}_{K,F}(a_i a_j) \end{aligned}$$

si ha

1. $\Delta^2 = \det T$
2. $\begin{cases} F \preceq K \text{ di Galois} \\ \text{ch} F = 0 \end{cases} \Rightarrow \Delta \neq 0$

Proof:

⟨1⟩ Dim 1.

$$\begin{aligned}\Delta^2 &= \det A \det A \underbrace{=}_{\text{prop. determinanti}} \det {}^t A \det A \underbrace{=}_{\text{Binet}} \det {}^t A A \\ ({}^t A A)_{ij} &= \sum_{k=1}^n ({}^t A)_{ik} A_{kj} = \sum_{k=1}^n A_{ki} A_{kj} = \sum_{k=1}^n \sigma_k(a_i) \sigma_k(a_j) \underbrace{=}_{\sigma \text{ omom.}} \sum_{k=1}^n \sigma_k(a_i a_j) = \text{Tr}(a_i a_j) = T_{ij} \\ &\Rightarrow {}^t A A = T\end{aligned}$$

$$\Delta^2 = \det {}^t A \det A = \det T$$

⟨2⟩ Dim 2.

Poiche' $\Delta \in \overline{F}$,

$$\Delta^2 \neq 0 \Leftrightarrow \Delta \neq 0$$

Consideriamo la funzione

$$\tau : K_F \times K_F \longrightarrow F$$

$$\tau(a, b) = \text{Tr}_{K, F}(ab)$$

⟨2.1⟩ τ e' ben posta

$$F \preceq K \text{ di Galois} \underbrace{\Rightarrow}_{[7.9, \text{pg. } 147]} \text{Tr}_{K, F}(\alpha) \in F \quad \forall \alpha \in K$$

⟨2.2⟩ τ e' una forma bilineare sullo spazio vettoriale K_F (vedi [GII, 2, pg. 32])

$$\begin{aligned}\tau(a + b, c) &= \text{Tr}((a + b)c) = \sum_{\sigma \in \mathcal{I}(K, F)} \sigma((a + b)c) = \sum_{\sigma \in \mathcal{I}(K, F)} \sigma(ac) + \sigma(bc) = \\ &= \sum_{\sigma \in \mathcal{I}(K, F)} \sigma(ac) + \sum_{\sigma \in \mathcal{I}(K, F)} \sigma(bc) = \tau(a, c) + \tau(b, c) \\ \tau(a, b + c) &= \tau(a, b) + \tau(a, c) \\ \mu \in F, \quad \mu \tau(a, b) &= \sum_{\sigma \in \mathcal{I}(K, F)} \mu \sigma(ab) \underbrace{=}_{\sigma|_F = \text{id}} \sum_{\sigma \in \mathcal{I}(K, F)} \sigma(\mu ab) = \tau(\mu a, b) = \tau(a, \mu b)\end{aligned}$$

⟨2.3⟩ T e' la matrice associata a τ rispetto alla base B

$$\tau(a_i, a_j) = \text{Tr}(a_i a_j) = T_{ij}$$

⟨2.4⟩ τ e' non degenerare

Usiamo la caratterizzazione [GII, 2.18, pg. 38]:

Sia $\alpha \in K_F$, $\alpha \neq 0$

$$\tau(\alpha, \alpha^{-1}) = \text{Tr}(\alpha \alpha^{-1}) = \text{Tr}(1) = \sum_{\sigma \in \mathcal{I}(K, F)} \sigma(1) \underbrace{=}_{\sigma|_F = \text{id}} \sum_{\sigma \in \mathcal{I}(K, F)} 1 = |\mathcal{I}(K, F)| =$$

$$\underbrace{=}_{F \preceq K \text{ di Galois}} [K : F] = n \underbrace{\neq}_{\text{ch } F = 0} 0$$

⟨2.5⟩ Q.E.D.

$$\tau \text{ non degenerare, } T \text{ matrice associata a } \tau \Rightarrow \det T \neq 0 \underbrace{\Leftrightarrow}_{\text{passo 1}} \Delta^2 \neq 0 \Leftrightarrow \Delta \neq 0$$

□

Proposition 7.12. Ponendoci nel contesto della def [7.10,pg.147], si ha

$$\begin{cases} F \preceq K \text{ di Galois} \\ \text{ch}F = 0 \end{cases} \Rightarrow \sigma_1, \dots, \sigma_n \text{ sono l.i. su } F, \text{ ovvero } \begin{cases} \sigma_1, \dots, \sigma_n \in \text{Hom}(K, F) = \text{spazio duale di } K_F \\ \mathcal{L}(\sigma_1, \dots, \sigma_n)_F = \text{Hom}(K, F) \end{cases}$$

Proof:

$$F \preceq K \text{ Galois} \xRightarrow{[6.24, \text{pg.96}]} \mathcal{G}(K, F) = \mathcal{I}(K, F) = \{\sigma_1, \dots, \sigma_n\}$$

$$\mathcal{G}(K, F) \xrightarrow{[6.3, \text{pg.78}]} \subseteq \text{Hom}(K, F)$$

$$\begin{cases} F \preceq K \text{ Galois} \\ \text{ch}F = 0 \end{cases} \Rightarrow \Delta \neq 0$$

Consideriamo una c.l. degli σ_i : $a_1\sigma_1 + \dots + a_n\sigma_n$ con $a_1, \dots, a_n \in F$. Dimostriamo che $a_1\sigma_1 + \dots + a_n\sigma_n = 0 \Leftrightarrow a_1 = a_2 = \dots = a_n = 0$

Sia dato il seguente sistema omogeneo nelle incognite $a_1, \dots, a_n$

$$\begin{cases} a_1\sigma_1(a_1) + \dots + a_n\sigma_n(a_1) = 0 \\ \dots \\ a_1\sigma_1(a_n) + \dots + a_n\sigma_n(a_n) = 0 \end{cases}$$

la sua matrice dei coefficienti e' proprio ${}^tA$ e quindi

$\det {}^tA = \det A = \Delta \neq 0 \Rightarrow$ ammette un'unica soluzione, quella nulla $\Rightarrow a_1 = a_2 = \dots = a_n = 0$ $\square$

Proposition 7.13. Sia

1. $F \preceq K$ di Galois, $\text{ch}F = 0$, con $n = [K : F]$
2. $G = \mathcal{G}(K, F) = \langle \tau \rangle$

allora, preso $\alpha \in K$, si ha

$$\mathcal{N}_{K,F}(\alpha) = 1 \Leftrightarrow \exists b \in K^* : \alpha = \frac{b}{\tau(b)}$$

Proof: Intanto osserviamo che

$$F \preceq K \text{ di Galois} \Rightarrow \begin{cases} \mathcal{I}(K, F) = G = \langle \tau \rangle \\ |G| = [K : F] = n \end{cases}$$

(1) Dim $\Leftarrow$

$$\begin{aligned}
G = \langle \tau \rangle & \underbrace{=}_{|G|=n} \{ \tau^0 = \text{id}, \tau, \dots, \tau^{n-1} \} \Rightarrow \mathcal{N}(\alpha) = \prod_{i=0}^{n-1} \tau^i(\alpha) \\
\tau^0(\alpha) = \alpha &= \frac{b}{\tau(b)} \\
\tau(\alpha) &= \frac{\tau(b)}{\tau^2(b)} \\
\tau^2(\alpha) &= \frac{\tau^2(b)}{\tau^3(b)} \\
&\dots \\
\tau^{n-1}(\alpha) &= \frac{\tau^{n-1}(b)}{\tau^n(b)} = \frac{\tau^{n-1}(b)}{b} \\
&\Rightarrow \prod_{i=0}^{n-1} \tau^i(\alpha) = \frac{b\tau(b)\tau^2(b)\dots\tau^{n-1}(b)}{\tau(b)\tau^2(b)\dots\tau^{n-1}(b)b} = 1
\end{aligned}$$

(2) Dim $\Rightarrow$

$$\begin{cases} F \preceq K \text{ di Galois, } \text{ch} F = 0 \\ G = \langle \tau \rangle \end{cases} \underbrace{\Rightarrow}_{[7.12, \text{pg.148}]} \tau^0 = \text{id}, \tau, \dots, \tau^{n-1} \text{ sono l.i. su } F \quad (1)$$

Sia $\varphi = \tau^0 + \alpha\tau + \alpha\tau(\alpha)\tau^2 + \dots + \alpha\tau(\alpha)\dots\tau^{n-2}(\alpha)\tau^{n-1} \in \text{Hom}(K, F)$

φ e' una c.l. di $\tau^0, \dots, \tau^{n-1}$ i cui coeff. non sono tutti nulli: $(1, \alpha, \alpha\tau(\alpha), \dots, \alpha\tau(\alpha)\dots\tau^{n-2}(\alpha)) \Rightarrow$

$$\underbrace{\varphi \neq 0}_{(1)} \Rightarrow \exists c \in K : \varphi(c) \neq 0$$

$$c \neq 0, \text{ infatti, } \varphi(0) = 0 + \alpha\tau(0) + \dots \underbrace{=}_{\tau|_F = \text{id}} 0$$

Sia $b = \varphi(c)$

$$\alpha = \frac{b}{\tau(b)} \Leftrightarrow \alpha\tau(b) = b \Leftrightarrow \alpha\tau(\varphi(c)) = b = \varphi(c)$$

$$\varphi(c) = c + \alpha\tau(c) + \alpha\tau(\alpha)\tau^2(c) + \dots + \alpha\tau(\alpha)\dots\tau^{n-2}(\alpha)\tau^{n-1}(c)$$

$$\alpha\tau(\varphi(c)) = \alpha\tau(c) + \alpha\tau(\alpha)\tau^2(c) + \alpha\tau(\alpha)\tau^2(\alpha)\tau^3(c) + \dots + \underbrace{\alpha\tau(\alpha)\tau^2(\alpha)\dots\tau^{n-1}(\alpha)}_{=\mathcal{N}(\alpha)=1} \underbrace{\tau^n(c)}_{=c} = \varphi(c) \Leftrightarrow$$

$$\Leftrightarrow \alpha\tau(c) + \alpha\tau(\alpha)\tau^2(c) + \alpha\tau(\alpha)\tau^2(\alpha)\tau^3(c) + \dots + \alpha\tau(\alpha)\tau^2(\alpha)\dots\tau^{n-2}(\alpha)\tau^{n-1}(c) + c = \varphi(c) \Leftrightarrow \text{vero} \quad \square$$

Proposition 7.14. Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unita'.

$$\begin{cases} F \preceq K \text{ di Galois, } \text{ch} F = 0, [K : F] = n \\ G = \mathcal{G}(K, F) = \langle \tau \rangle \\ \omega \in F \end{cases} \Leftrightarrow \exists b \in K^* : K = F(b) = CS(x^n - b^n, F), b^n \in F$$

Proof:

$$\begin{aligned}
\omega \in F, U_n = \langle \omega \rangle &\xRightarrow[F \text{ campo}]{} U_n \subseteq F \\
\tau(\omega^{-1}) &\xRightarrow[\tau|_F = \text{id}, \omega^{-1} \in F]{} = \omega^{-1} \quad (*) \\
\mathcal{N}(\omega^{-1}) &\xRightarrow[G = \langle \tau \rangle]{} \prod_{i=0}^{n-1} \tau^i(\omega^{-1}) \xRightarrow{(*)} \prod_{i=0}^{n-1} \omega^{-1} = \omega^{-n} = 1 \\
\mathcal{N}(\omega^{-1}) = 1 &\xRightarrow{[7.13, \text{pg.149}]} \exists b \in K^* : \omega^{-1} = \frac{b}{\tau(b)} \Leftrightarrow \tau(b) = \omega b \quad (1) \\
\tau^{i+1}(b) = \tau^i(\tau(b)) &\xRightarrow{(1)} \tau^i(\omega) \tau^i(b) = \omega \omega^i b = \omega^{i+1} b \\
\Rightarrow \tau^i(b) = \omega^i b \neq b \quad \forall i = 1, \dots, n-1 &\Leftrightarrow g(b) \neq b \quad \forall g \in G \setminus \{\text{id}\} \Leftrightarrow \\
&\Leftrightarrow (g(b) = b \Rightarrow g = \text{id}) \quad (2)
\end{aligned}$$

(1) $K = F(b)$

$$\begin{aligned}
F \preceq F(b) \preceq K &\xRightarrow{Corrispondenza[6.25, \text{pg.96}]} H = \mathcal{G}(K, F(b)) \leq G \\
F \preceq K \text{ Galois} &\xRightarrow{[6.23, \text{pg.96}]} F(b) \preceq K \text{ Galois} \xRightarrow{[6.19, \text{pg.92}]} F(b) = K^{\mathcal{G}(K, F(b))} = K^H \\
b \in F(b) = K^H &\Rightarrow h(b) = b \quad \forall h \in H \leq G \xRightarrow{(2)} h = \text{id} \quad \forall h \in H \Leftrightarrow H = \{\text{id}\} \\
F(b) \preceq K \text{ Galois} &\xRightarrow{[6.19, \text{pg.92}]} [K : F(b)] = |\mathcal{G}(K, F(b))| = |H| = 1
\end{aligned}$$

$$\begin{cases} F(b) \subseteq K \\ \dim K_{F(b)} = 1 \end{cases} \Rightarrow F(b) = K$$

(2) $b^n \in F$

$$\begin{aligned}
\tau(b^n) = \tau(b)^n &\xRightarrow{(1)} \omega^n b^n \xRightarrow{\omega^n = 1} b^n \\
\Rightarrow \tau^i(b^n) = b^n \quad \forall i = 0, 1, \dots, n-1 &\Rightarrow b^n \in K^G \xRightarrow{F \preceq K \text{ di Galois}} F
\end{aligned}$$

(3) $F(b) = CS(x^n - b^n, F)$

Le radici di $x^n - b^n$ sono (vedi [1.19, pg.7])

$$b, \omega b, \omega^2 b, \dots, \omega^{n-1} b$$

quindi

$$CS(x^n - b^n, F) = F(b, \omega b, \omega^2 b, \dots, \omega^{n-1} b) \xRightarrow{\omega \in F} F(b)$$

□

Proposition 7.15. Sia data l'estensione $F \preceq K$ e sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime

dell'unità',

$$\begin{cases} K = CS(x^n - a, F), & a \in F^* \\ \omega \in F, & \text{ch} F = 0 \end{cases} \Rightarrow \begin{cases} F \preceq K \text{ e' di Galois} \\ G = \mathcal{G}(K, F) \text{ e' ciclico} \\ [K : F] / n \end{cases}$$

Proof: Le radici di $f(x) = x^n - a$ sono (vedi [1.19,pg.7])

$$b, \omega b, \omega^2 b, \dots, \omega^{n-1} b \in CS(x^n - a, F) = K$$

dove $b = \sqrt[n]{a}$

Nota: $a \in F^* \Rightarrow a \neq 0 \Rightarrow b \neq 0$

$$f(x) \underbrace{=}_{b^n=a} x^n - b^n, \text{ ch} F = 0, \quad b^n = a \neq 0 \quad \Rightarrow \quad f(x) \text{ separabile} \quad [6.41, \text{pg.112}]$$

(1) $F \preceq K$ e' di Galois

$$\begin{cases} f(x) \text{ separabile} \\ K = CS(x^n - a, F) \end{cases} \Rightarrow F \preceq K \text{ di Galois} \quad [6.19, \text{pg.92}]$$

(2) $F \preceq K$ e' semplice

$$K = CS(x^n - a, F) = F(b, \omega b, \omega^2 b, \dots, \omega^{n-1} b) \underbrace{=}_{\omega = \frac{\omega b}{b}} F(b, \omega) \underbrace{=}_{\omega \in F} F(b)$$

Sia $\varphi \in G = \mathcal{G}(K, F)$

$$\begin{cases} K = CS(f(x), F) \\ f(x) \text{ separabile} \\ A = \{b, \omega b, \dots, \omega^{n-1} b\} \text{ radici di } f(x) \end{cases} \Rightarrow \varphi|_A \in S_n(A) \Rightarrow \varphi(b) \in A \Leftrightarrow \exists i : \varphi(b) = \omega^i b \quad (1) \quad [6.26, \text{pg.99}]$$

Definiamo allora la seguente applicazione:

$$\phi : G \longrightarrow U_n$$

$$\varphi \mapsto \frac{\varphi(b)}{b}$$

$$\phi \text{ e' ben definita perche' } b \neq 0, \text{ e per la (1) } \exists i : \frac{\varphi(b)}{b} = \omega^i$$

(3) ϕ e' un omomorfismo di gruppi

Siano $\varphi_1, \varphi_2 \in G$, con $\varphi_1(b) = \omega^i b$, $\varphi_w(b) = \omega^j b$, si ha

$$\varphi_1 \varphi_2(b) = \varphi_1(\omega^j b) = \varphi(\omega)^j \varphi(b) \underbrace{=}_{\varphi_2|_F = \text{id}, \omega \in F} \omega^j \varphi_1(b) = \omega^j \omega^i b = \omega^{i+j} b$$

$$\phi(\varphi_1 \varphi_2) = \frac{\varphi_1 \varphi_2(b)}{b} = \omega^{i+j}$$

$$\phi(\varphi_1) \phi(\varphi_2) = \frac{\varphi_1(b)}{b} \frac{\varphi_2(b)}{b} = \omega^i \omega^j = \omega^{i+j} = \phi(\varphi_1 \varphi_2)$$

(4) ϕ e' iniettiva

$$\begin{aligned}
\ker \phi &= \left\{ \varphi \in G \mid \frac{\varphi(b)}{b} = 1 \Leftrightarrow \varphi(b) = b \right\} \\
K = F(b) &= \{a_0 + a_1 b + \dots + a_r b^r \mid a_i \in F\}, \quad \varphi(a_0 + a_1 b + \dots + a_r b^r) \underbrace{=}_{\varphi|_F = \text{id}} a_0 + a_1 \varphi(b) + \dots + a_r \varphi(b)^r = \\
&\underbrace{=}_{\varphi(b)=b} a_0 + a_1 b + \dots + a_r b^r \Rightarrow (\varphi(b) = b \Rightarrow \varphi = \text{id}_K) \\
&\Rightarrow \ker \phi = \{\text{id}_K\} \Rightarrow \phi \text{ iniettiva} \\
(5) \text{ Q.E.D.}
\end{aligned}$$

$$\begin{aligned}
\phi \text{ iniettiva} &\Rightarrow G \simeq \text{Im } \phi \leq U_n \xRightarrow{\text{Lagrange [AII, 1.53, pg. 19]}} |G|/|U_n| \underbrace{=}_{[6.41, \text{pg. 112}]} n \\
F \preceq K \text{ di Galois} &\xRightarrow{[6.19, \text{pg. 92}]} |G| = [K : F] \Rightarrow [K : F]/n \\
\begin{cases} U_n = \langle \omega \rangle \text{ ciclico} \\ \text{Im } \phi \leq U_n \end{cases} &\xRightarrow{[AII, 1.39, \text{pg. 13}]} \text{Im } \phi \simeq G \text{ ciclico}
\end{aligned}$$

□

Definition 7.16. Sia $F \preceq K$ una estensione algebrica.

$$F \preceq K \text{ e' ciclica} \stackrel{\text{def}}{\Leftrightarrow} \mathcal{G}(K, F) \text{ e' ciclico}$$

Theorem 7.17. *Sia*

1. $U_n = \langle \omega \rangle$
2. $F \preceq K$ una estensione, con $\text{ch} F = 0$, $\omega \in F$

allora

$$K = F(b), \quad b^n \in F^* \Leftrightarrow \begin{cases} F \preceq K \text{ e' ciclica e di Galois} \\ [K : F]/n \end{cases}$$

Proof:

(1) $\text{Dim} \Rightarrow$

$$\begin{aligned}
CS(x^n - b^n, F) &\underbrace{=}_{[1.19, \text{pg. 7}]} F(b, \omega b, \omega^2 b, \dots, \omega^{n-1} b) \underbrace{=}_{\omega = \frac{\omega b}{b}} F(\omega, b) \underbrace{=}_{\omega \in F} F(b) \\
\begin{cases} K = F(b) = CS(x^n - b^n, F), \quad b^n \in F^* \\ \omega \in F, \quad \text{ch} F = 0 \end{cases} &\xRightarrow{[7.15, \text{pg. 151}]} \begin{cases} F \preceq K \text{ e' di Galois} \\ G = \mathcal{G}(K, F) \text{ e' ciclico} \\ [K : F]/n \end{cases}
\end{aligned}$$

cioe' la tesi.

(2) $\text{Dim} \Leftarrow$

$$\begin{aligned}
m &= [K : F] / n \Rightarrow m\lambda = n \\
\omega \in F, U_n &= \langle \omega \rangle \Rightarrow U_n \subseteq F \\
x^m = 1 &\Rightarrow (x^m)^\lambda = 1 \Leftrightarrow x^n = 1 \\
&\Rightarrow U_m \leq U_n \subseteq F \\
\text{Sia } \omega' \text{ t.c. } U_m &= \langle \omega' \rangle \\
\begin{cases} F \preceq K \text{ di Galois, } \text{ch} F = 0, [K : F] = m \\ F \preceq K \text{ e' ciclica} \\ \omega' \in U_m \subseteq F \end{cases} &\stackrel{\Rightarrow}{\underset{[7.14, \text{pg.150}]}{}} \exists b \in K^* : K = F(b), b^n \in F
\end{aligned}$$

che e' la tesi. □

Proposition 7.18. *Sia F campo con $\text{ch} F = 0$ e sia $U_n = \langle \omega \rangle$, allora*

1. $F \preceq F(\omega)$ e' di Galois
2. $\mathcal{G}(F(\omega), F) \hookrightarrow (U(\mathbb{Z}_n), \cdot)$
3. $\mathcal{G}(F(\omega), F)$ abeliano

dove $(U(\mathbb{Z}_n), \cdot)$ e' il gruppo moltiplicativo degli invertibili di $\mathbb{Z}_n$.

Proof:

(1) Dim. 1.

$$\begin{cases} F(\omega) = CS(x^n - 1, F) \\ \text{ch} F = 0, 1 \neq 0 \end{cases} \stackrel{\Rightarrow}{\underset{[6.41, \text{pg.112}]}{}} x^n - 1 \text{ separabile} \stackrel{\Rightarrow}{\underset{[6.19, \text{pg.92}]}{}} F \preceq F(\omega) \text{ di Galois}$$

(2) Dim 2.

Si procede analogamente alla prop. [6.43,pg.118], considerando pero' che

$$\text{ch} F = 0 \Rightarrow \mathbb{Q} \preceq F \Rightarrow P_{\min}(\omega, F) / P_{\min}(\omega, \mathbb{Q})$$

e quindi non vale la surriettivita'. L'iniettivita' continua a valere, quindi

$$\mathcal{G}(F(\omega), F) \hookrightarrow (U(\mathbb{Z}_n), \cdot)$$

(3) Dim 3.

$U(\mathbb{Z}_n)$ e' un gruppo abeliano, quindi ogni suo sottogruppo e' abeliano. □

Proposition 7.19. *Sia*

1. F campo, $\text{ch} F = 0$
2. $K = CS(x^n - a, F)$, $a \in F^*$

allora

$$\mathcal{G}(K, F) \text{ e' risolubile}$$

Proof: Per la prop [6.41,pg.112], $x^n - a$ e' separabile e le sue radici distinte sono

$$b, \omega b, \dots, \omega^{n-1} b$$

$$b \in K, b^n = a, U_n = \langle \omega \rangle$$

$$a \neq 0 \Rightarrow b \neq 0$$

quindi

$$K = CS(x^n - a, F) = F(b, \omega b, \dots, \omega^{n-1}b) \underbrace{=}_{\omega = \frac{\omega b}{b}} F(b, \omega)$$

Sia $G = \mathcal{G}(K, F)$, $H = \mathcal{G}(K, F(\omega))$, $J = \mathcal{G}(F(\omega), F)$

$$\text{ch}F = 0, U_n = \langle \omega \rangle \underbrace{\Rightarrow}_{[7.18, \text{pg.154}]} \begin{cases} F \preceq F(\omega) \text{ di Galois} \\ J \text{ e' abeliano} \end{cases} \quad (1)$$

$$\begin{cases} x^n - a \text{ separabile} \\ K = CS(x^n - a, F) \end{cases} \Rightarrow F \preceq K \text{ di Galois}$$

$$\begin{cases} U_n = \langle \omega \rangle \\ K = F(\omega)(b), \text{ ch}F(\omega) = \text{ch}F = 0, \omega \in F(\omega) \\ b^n = a \in F^* \subseteq F(\omega)^* \end{cases} \underbrace{\Rightarrow}_{[7.17, \text{pg.153}]} F(\omega) \preceq K \text{ e' ciclica}$$

$$F(\omega) \preceq K \text{ ciclica} \underbrace{\Rightarrow}_{\text{per def.}} H = \mathcal{G}(K, F(\omega)) \text{ ciclico} \Rightarrow H \text{ abeliano} \quad (2)$$

$$\begin{cases} F \preceq K \text{ di Galois} \\ (1) \Rightarrow F \preceq F(\omega) \text{ Galois} \end{cases} \underbrace{\Rightarrow}_{[6.30, \text{pg.101}]} \begin{cases} \frac{G}{H} \simeq J \text{ che e' abeliano} \\ H \leq G \text{ normale} \end{cases} \quad (1.1)$$

Per la (2) e (1.1), la seguente catena

$$\{\mathbf{e}\} \leq H \leq G$$

e' risolvente per G . □

Proposition 7.20. *Sia*

1. $F \preceq K$ una estensione di Galois, con $\text{ch}F = 0$
2. $U_n = \langle \omega \rangle$

Allora,

1. $F(\omega) \preceq K(\omega)$ e' di Galois
2. $\mathcal{G}(K(\omega), F(\omega)) \hookrightarrow \mathcal{G}(K, F)$
3. $\mathcal{G}(K, F)$ risolubile $\Leftrightarrow \mathcal{G}(K(\omega), F(\omega))$ risolubile

Proof:

(1) Dim 1.

$$F \preceq K \text{ di Galois} \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} \exists f(x) \in F[x] \text{ separabile t.c. } K = CS(f(x), F) = F(\beta_1, \dots, \beta_m)$$

$$K(\omega) = F(\omega, \beta_1, \dots, \beta_m) = CS(f(x), F(\omega))$$

$$\begin{cases} f(x) \text{ separabile} \\ K(\omega) = CS(f(x), F(\omega)) \end{cases} \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]} F(\omega) \preceq K(\omega) \text{ di Galois}$$

(2) Dim 2.

Consideriamo la seguente applicazione:

$$\phi : \mathcal{G}(K(\omega), F(\omega)) \longrightarrow \mathcal{G}(K, F)$$

$$\varphi \mapsto \varphi|_K$$

⟨2.1⟩ ϕ e' ben posta

$$\begin{aligned}
F \preceq K \text{ Galois} &\Rightarrow \mathcal{G}(K, F) = \mathcal{I}(K, F) \\
\begin{cases} F \preceq K \preceq K(\omega) \\ F \preceq K, \quad K \preceq K(\omega) \text{ algebriche} \end{cases} &\xRightarrow{[2.45, \text{pg.31}]} F \preceq K(\omega) \text{ algebrica} \xRightarrow{[2.62, \text{pg.49}]} \overline{F} = \overline{K(\omega)} \\
\varphi \in \mathcal{G}(K(\omega), F(\omega)) &\Rightarrow \text{Im } \varphi|_K \subseteq K(\omega) \subseteq \overline{K(\omega)} = \overline{F} \\
\begin{cases} \varphi|_K : K \longrightarrow \overline{F} \\ \varphi|_F = \text{id} \\ \varphi|_K \text{ omomorfismo} \end{cases} &\Rightarrow \varphi|_K \in \mathcal{I}(K, F) = \mathcal{G}(K, F)
\end{aligned}$$

⟨2.2⟩ ϕ e' un omomorfismo

$$\begin{aligned}
\phi(fg) &= (fg)|_K \\
\phi(g) \in \mathcal{G}(K, F) &\Leftrightarrow g|_K \in \mathcal{G}(K, F) \Rightarrow \text{Im } g|_K \subseteq K \\
\phi(f)\phi(g) &= f|_K g|_K \xRightarrow{\text{Im } g|_K \subseteq K} (fg)|_K = \phi(fg)
\end{aligned}$$

⟨2.3⟩ ϕ e' iniettiva

$$\begin{aligned}
\ker \phi &= \{\varphi \in \mathcal{G}(K(\omega), F(\omega)) \mid \varphi|_K = \text{id}\} \\
\begin{cases} \varphi \in \mathcal{G}(K(\omega), F(\omega)) \Rightarrow \varphi|_{F(\omega)} = \text{id} \\ \varphi|_K = \text{id} \end{cases} &\quad (1) \\
K(\omega) &= \{a_0 + a_1\omega + \dots + a_r\omega^r \mid a_i \in K\} \\
\varphi(a_0 + a_1\omega + \dots + a_r\omega^r) &\xRightarrow{\varphi|_K = \text{id}} = a_0 + a_1\varphi(\omega) + \dots + a_r\varphi(\omega)^r \xRightarrow{\varphi|_{F(\omega)} = \text{id}} = a_0 + a_1\omega + \dots + a_r\omega^r \\
&\Rightarrow \varphi = \text{id} \\
\ker \phi &= \{\text{id}\} \Rightarrow \phi \text{ iniettiva}
\end{aligned}$$

⟨3⟩ Dim. 3.

⟨3.1⟩ Dim. $\Rightarrow$

$$\begin{aligned}
\text{passo 2} &\Rightarrow \mathcal{G}(K(\omega), F(\omega)) \simeq H \leq \mathcal{G}(K, F) \\
\begin{cases} \mathcal{G}(K, F) \text{ risolubile} \\ H \leq \mathcal{G}(K, F) \end{cases} &\xRightarrow{[7.3, \text{pg.140}]} H \text{ risolubile}
\end{aligned}$$

⟨3.1⟩ Dim. $\Leftarrow$

⟨3.1.1⟩ Dimostriamo intanto che $F \preceq K(\omega)$ e' di Galois.

$$\begin{aligned}
& \left\{ \begin{array}{l} \text{ch} F = 0 \\ F \preceq K(\omega) \text{ algebrica} \end{array} \right. \underbrace{\Rightarrow}_{[3.23, \text{pg.} 60]} F \preceq K(\omega) \text{ separabile} \\
& F \preceq K \text{ Galois} \Rightarrow F \preceq K \text{ finita} \\
& K \preceq K(\omega) \text{ algebrica e fin. gen.} \underbrace{\Rightarrow}_{[2.44, \text{pg.} 31]} K \preceq K(\omega) \text{ finita} \\
& F \preceq K, K \preceq K(\omega) \text{ finite} \underbrace{\Rightarrow}_{[2.18, \text{pg.} 16]} F \preceq K(\omega) \text{ finita} \\
& F \preceq K(\omega) \text{ separabile e finita} \underbrace{\Rightarrow}_{[6.10, \text{pg.} 84]} |\mathcal{I}(K(\omega), F)| = [K(\omega) : F] \quad (3)
\end{aligned}$$

(3.1.1.1) $\text{Dim } \mathcal{I}(K(\omega), F) = \mathcal{G}(K(\omega), F)$

Per la prop [6.4, pg. 79] abbiamo gia' l'inclusione $\supseteq$. Dimostriamo la $\subseteq$.

Sia $\varphi \in \mathcal{I}(K(\omega), F)$.

(3.1.1.1.1) $\text{Dim Im } \varphi \subseteq K(\omega)$

$$\begin{aligned}
K(\omega) &= \{a_0 + a_1\omega + \cdots + a_r\omega^r \mid a_i \in K\} \\
\varphi(a_0 + a_1\omega + \cdots + a_r\omega^r) &= \sum_{i=0}^r \varphi(a_i)\varphi(\omega)^i
\end{aligned}$$

Analogamente a quanto visto nel passo 2 abbiamo:

$$\begin{aligned}
& \left\{ \begin{array}{l} \text{Im } \varphi|_K \subseteq \overline{F} \\ \varphi|_K \text{ omomorfismo} \\ \varphi|_F = \text{id} \end{array} \right. \Rightarrow \varphi|_K \in \mathcal{I}(K, F) = \mathcal{G}(K, F) \Rightarrow \varphi|_K : K \longrightarrow K \Rightarrow \varphi(a_i) \in K \\
& \left\{ \begin{array}{l} \text{Im } \varphi|_{F(\omega)} \subseteq \overline{F} \\ \varphi|_{F(\omega)} \text{ omomorfismo} \\ \varphi|_F = \text{id} \end{array} \right. \Rightarrow \varphi|_{F(\omega)} \in \mathcal{I}(F(\omega), F) \underbrace{\Rightarrow}_{F \preceq F(\omega) \text{ di Galois per la prop [7.18, pg. 154]}} \\
& \quad = \mathcal{G}(F(\omega), F) \Rightarrow \text{Im } \varphi|_{F(\omega)} \subseteq F(\omega) \Rightarrow \varphi(\omega) \in F(\omega) \\
& \Rightarrow \varphi(a_i)\varphi(\omega) \in K \cup F(\omega) \subseteq K(\omega) \Rightarrow \text{Im } \varphi \subseteq K(\omega)
\end{aligned}$$

Quindi

$$\begin{aligned}
& \left\{ \begin{array}{l} \varphi \in \mathcal{I}(K(\omega), F) \\ \text{Im } \varphi \subseteq K(\omega) \end{array} \right. \underbrace{\Rightarrow}_{[6.3, \text{pg.} 78]} \varphi \text{ endomorfismo iniettivo} \Rightarrow \\
& \underbrace{\Rightarrow}_{[AL, 8.1, \text{pg.} 50]} \varphi \text{ isomorfismo vettoriale} \Rightarrow \varphi \text{ biettiva} \\
& \left\{ \begin{array}{l} \text{Im } \varphi \subseteq K(\omega) \\ \varphi \text{ omomorfismo} \\ \varphi|_F = \text{id} \\ \varphi \text{ biettiva} \end{array} \right. \Rightarrow \varphi \in \mathcal{G}(K(\omega), F)
\end{aligned}$$

Per l'arbitrarieta' di φ abbiamo cosi' dimostrato che $\mathcal{I}(K(\omega), F) \subseteq \mathcal{G}(K(\omega), F)$.

Ritornando alla (3):

$$\begin{aligned} |\mathcal{G}(K(\omega), F)| &\underset{\text{passo 3.1.1.1}}{=} |\mathcal{I}(K(\omega), F)| \underset{(3)}{=} [K(\omega) : F] \\ |\mathcal{G}(K(\omega), F)| &= [K(\omega) : F] \underset{[6.19, \text{pg. 92}]}{\Rightarrow} F \preceq K(\omega) \text{ di Galois} \end{aligned}$$

Concludiamo:

$\mathcal{G}(F(\omega), F)$ abeliano (vedi [7.18, pg. 154]) $\Rightarrow \mathcal{G}(F(\omega), F)$ risolubile (4)

$$\begin{cases} F \preceq K(\omega) \text{ di Galois (passo 3.1.1)} \\ F \preceq F(\omega) \text{ di Galois (vedi [7.18, pg. 154])} \\ F \preceq F(\omega) \preceq K(\omega) \\ F \preceq K \preceq K(\omega) \end{cases} \underset{[6.30, \text{pg. 101}]}{\Rightarrow} \begin{cases} \mathcal{G}(K, F) \simeq \frac{\mathcal{G}(K(\omega), F)}{\mathcal{G}(K(\omega), K)} \quad (5.1) \\ \mathcal{G}(F(\omega), F) \simeq \frac{\mathcal{G}(K(\omega), F)}{\mathcal{G}(K(\omega), F(\omega))} \quad (5.2) \end{cases}$$

$$(4), (5.2), \mathcal{G}(K(\omega), F(\omega)) \text{ risolubile per Hp} \underset{[7.4, \text{pg. 144}]}{\Rightarrow} \mathcal{G}(K(\omega), F) \text{ risolubile} \quad (5.3)$$

$$(5.1), (5.3) \underset{[7.3, \text{pg. 140}]}{\Rightarrow} \mathcal{G}(K, F) \text{ risolubile}$$

□

7.3 Estensioni risolubili per radicali

Definition 7.21. Sia $f(x) \in F[x]$, $L = CS(f(x), F)$,

$$f(x) \text{ e' risolubile per radicali} \stackrel{\text{def}}{\Leftrightarrow} \begin{cases} \exists K : L \preceq K = F(\alpha_1, \dots, \alpha_m) \\ \exists n_1 : \alpha_1^{n_1} \in F \\ \forall i = 2, \dots, m \exists n_i : \alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1}) \end{cases}$$

In altre parole, $f(x)$ e' risolubile per radicali, quando riusciamo a contenere il suo campo di spezzamento, estendendolo con elementi che sono radici di $x^{n_i} = a_i$, o piu' in dettaglio:

$$\begin{aligned} \alpha_1^{n_1} &= a_1 \in F \Leftrightarrow \alpha_1 = \sqrt[n_1]{a_1} \\ F &\preceq F(\alpha_1) \\ \alpha_2^{n_2} &= a_2 \in F(\alpha_1) \Leftrightarrow \alpha_2 = \sqrt[n_2]{a_2} \\ F &\preceq F(\alpha_1, \alpha_2) \\ &\dots \end{aligned}$$

L'estensione $F \preceq K$ e' l'estensione che risolve $f(x)$ per radicali.

Lemma 7.22. Sia

1. $f(x) \in F[x]$, $\text{ch} F = 0$
2. $K = CS(f(x), F)$

allora

$f(x)$ e' risolubile per radicali $\Rightarrow \exists F \preceq E$ estensione di Galois che risolve $f(x)$ per radicali, ovvero

$$\begin{cases} \exists E : CS(f(x), F) \preceq E = F(\alpha_1, \dots, \alpha_m) \\ \forall i = 1, \dots, m \exists n_i : \alpha_i^{n_i} \in F_{i-1} \\ F_0 = F, \quad F_i = F_{i-1}(\alpha_i) \quad \forall i = 1, \dots, m \\ F \preceq E \text{ di Galois} \end{cases}$$

Proof: Poiche' $f(x)$ e' risolubile per radicali, si ha

$$\begin{aligned} \exists E : K \preceq E &= F(\alpha_1, \dots, \alpha_m) \\ \forall i = 1, \dots, m \exists n_i : \alpha_i^{n_i} &\in F_{i-1} \quad (1) \\ F_0 &= F, \quad F_i = F_{i-1}(\alpha_i) \quad \forall i = 1, \dots, m \end{aligned}$$

PROOF SKETCH: Aggiungeremo adesso altri α_i in modo da avere una estensione piu' grande, risolvente e di Galois

Siano $\sigma_1, \dots, \sigma_t$ gli elementi distinti di $\mathcal{I}(E, F)$. Sia $m' : m < m' + 1 \leq t$. Dividiamo m' per m , $m' = hm + i$, $0 \leq i < m$ e poniamo

$$\alpha_{m'+1} = \alpha_{hm+i+1} = \sigma_h(\alpha_{i+1})$$

Poniamo infine

$$\begin{aligned} E_0 &= F \\ E_{i+1} &= E_i(\alpha_{i+1}) \quad \forall i = 0, \dots, t-1 \end{aligned}$$

La catena $E_0 \preceq E_1 \preceq \dots \preceq E_t$, ovvero,

$$\begin{aligned} F \preceq F(\alpha_1) \preceq F(\alpha_1, \alpha_2) \preceq \dots \preceq F(\alpha_1, \dots, \alpha_m) &= E = E_m \preceq \\ \preceq E_{m+1} = E_m(\sigma_1(\alpha_1)) \preceq E_{m+1}(\sigma_1(\alpha_2)) \preceq \dots \preceq E_{t-1}(\alpha_t) &= E_t \end{aligned}$$

e' ancora una catena che risolve per radicali $f(x)$. Infatti, $E_t \supseteq E_m = E \supseteq K$, la prop (1) vale per tutto il pezzo $E_0 \preceq \dots \preceq E_m = E$.

(0.1) Dimostriamo che la (1) vale anche per $E_{m+1} \preceq \dots \preceq E_t$, ovvero che

$$\forall j = m+1, \dots, t \exists n_j : \alpha_j^{n_j} \in E_{j-1}$$

Sia $j : m < j \leq t$. Dividiamo $j-1$ per m , $j-1 = hm + i'$, $i' < m$. Sia $i = i' + 1$, si ha

$$\begin{aligned} \alpha_j &= \sigma_h(\alpha_i) \\ i \leq m \Rightarrow \alpha_i^{n_i} \in F_{i-1} &\Rightarrow \sigma_h(\alpha_i^{n_i}) \in \sigma_h(F(\alpha_1, \dots, \alpha_{i-1})) \quad \underbrace{=} \quad F(\sigma_h(\alpha_1), \dots, \sigma_h(\alpha_{i-1})) \subseteq E_{j-1} \end{aligned}$$

[6.34,pg.106]

$$\alpha_j^{n_i} = \sigma_h(\alpha_i)^{n_i} \quad \underbrace{=}_{\sigma_h \text{ omomo.}} \quad \sigma_h(\alpha_i^{n_i}) \in E_{j-1}$$

Quindi basta scegliere $n_j = n_i$.

(0.2) Dimostriamo che $F \preceq E_t$ e' di Galois

$$\begin{cases} \text{ch} F = 0 \\ F \preceq E_t \text{ algebrica} \end{cases} \quad \underbrace{\Rightarrow}_{[3.23, \text{pg.60}]} \quad F \preceq E_t \text{ e' separabile}$$

$$F \preceq E_t \text{ separabile e finita} \Rightarrow |\mathcal{I}(E_t, F)| = [E_t : F]$$

Dimostriamo che $\mathcal{I}(E_t, F) = \mathcal{G}(E_t, F)$. Per la prop [6.4,pg.79], l'inclusione $\supseteq$ e' vera.

Dimostriamo la $\subseteq$. Sia $\varphi \in \mathcal{I}(E_t, F)$

$$E_t = F(\alpha_1, \dots, \alpha_m, \sigma_h(\alpha_i) \quad \forall i, h : m < hm + i \leq t, \quad i < m) =$$

$$\underbrace{F(\sigma_h(\alpha_i) \quad \forall i, h : m < hm + i \leq t, \quad i < m)}_{\exists j' : \sigma_{j'} = \text{id}}$$

$$\varphi : E_t \longrightarrow \overline{F}$$

$$\sigma_h(E) = \sigma_h(F(\alpha_1, \dots, \alpha_m)) \underbrace{=}_{[6.34, \text{pg.} 106]} F(\sigma_h(\alpha_1), \dots, \sigma_h(\alpha_m)) \subseteq E_t$$

$$\Rightarrow \sigma_h : E \longrightarrow E_t$$

$$\varphi \circ \sigma_h : E \longrightarrow E_t \longrightarrow \overline{F}$$

$$\Rightarrow \varphi \sigma_h \in \mathcal{I}(E, F) \Rightarrow \exists j : \varphi \sigma_h = \sigma_j \quad (*)$$

$$\varphi(E_t) = F(\varphi \sigma_h(\alpha_i) \quad \forall i, h : m < hm + i \leq t, \quad ; \quad i < m) \underbrace{=}_{(*)} F(\sigma_{j_h}(\alpha_i) \quad \forall i, h : m < hm + i \leq t, \quad ; \quad i < m) \subseteq E_t$$

$$\Rightarrow \varphi : E_t \longrightarrow E_t \Rightarrow \varphi \in \mathcal{G}(E_t, F)$$

Quindi $\mathcal{I}(E_t, F) \subseteq \mathcal{G}(E_t, F)$

$$\mathcal{I}(E_t, F) = \mathcal{G}(E_t, F)$$

Allora,

$$|\mathcal{G}(E_t, F)| = |\mathcal{I}(E_t, F)| = [E_t : F] \underbrace{\Rightarrow}_{[6.19, \text{pg.} 92]} F \preceq E_t \text{ e' di Galois}$$

□

Theorem 7.23. *di Galois.*

Sia

$$1. f(x) \in F[x], \text{ ch } F = 0$$

$$2. K = CS(f(x), F)$$

allora

$$f(x) \text{ e' risolubile per radicali} \Leftrightarrow \mathcal{G}(K, F) \text{ e' risolubile}$$

Proof:

(1) Dim $\Leftarrow$

Per il thm [5.5, pg. 76], $F \preceq K$ e' finita. Sia $G = \mathcal{G}(K, F)$.

$$\begin{cases} \text{ch } F = 0 \\ K = CS(f(x), F) \end{cases} \underbrace{\Rightarrow}_{[6.22, \text{pg.} 96], [6.19, \text{pg.} 92]} \begin{cases} F \preceq K \text{ di Galois} \\ n = [K : F] = |G| = |\mathcal{G}(K, F)| \end{cases} \quad (1)$$

Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unita' (nel campo F).

$$\begin{cases} F \preceq K \text{ di Galois, ch } F = 0 \\ U_n = \langle \omega \rangle \\ \mathcal{G}(K, F) \text{ risolubile} \end{cases} \underbrace{\Rightarrow}_{[7.20, \text{pg.} 155]} \begin{cases} F(\omega) \preceq K(\omega) \text{ di Galois} \quad (2.1) \\ \mathcal{G}(K(\omega), F(\omega)) \simeq H \leq G \quad (2.2) \\ \mathcal{G}(K(\omega), F(\omega)) \text{ risolubile} \quad (2.3) \end{cases}$$

Sia $\Gamma = \mathcal{G}(K(\omega), F(\omega))$. Se $|\Gamma| = 1$, allora

$$1 = |\Gamma| \underbrace{=} [K(\omega) : F(\omega)] \Rightarrow K(\omega) = F(\omega)$$

$F(\omega) \preceq K(\omega)$ Galois

$$\begin{cases} CS(f(x), F) = K \preceq K(\omega) = F(\omega) \\ \omega^n = 1 \in F \end{cases} \underbrace{\Rightarrow}_{\text{per def.}} f(x) \text{ e' risol. per radicali}$$

Supponiamo adesso che $|\Gamma| > 1$.

$$\left\{ \begin{array}{l} (2.3) \\ 1 < |\Gamma| < +\infty \end{array} \right\} \xRightarrow{[7.3, \text{pg.140}]} \exists \text{ catena risolvnte } \{\text{id}\} = \Gamma_0 \leq \dots \leq \Gamma_m = \Gamma \text{ t.c. } \left| \frac{\Gamma_i}{\Gamma_{i-1}} \right| = p_i \text{ primo } \forall i \quad (3)$$

$$p_i = \left| \frac{\Gamma_i}{\Gamma_{i-1}} \right| = \frac{|\Gamma_i|}{|\Gamma_{i-1}|} \Leftrightarrow p_i |\Gamma_{i-1}| = |\Gamma_i| \Rightarrow p_i \Big/ \underbrace{|\Gamma_i|}_{\Gamma_i \leq \Gamma} \Big/ \underbrace{|\Gamma|}_{(2.2)} \Big/ \underbrace{|G|}_{(1)} = n$$

$$p_i \Big/ n \quad \forall i = 1, \dots, m \quad (3.1)$$

$$\left| \frac{\Gamma_i}{\Gamma_{i-1}} \right| = p_i \text{ primo} \Rightarrow \frac{\Gamma_i}{\Gamma_{i-1}} \text{ ciclico} \quad (3.2)$$

Sia $E_i = K(\omega)^{\Gamma_i}$. Per il thm di Corrispondenza di Galois (vedi [6.25,pg.96]), applicato alla catena (3), abbiamo

$$\langle 1.1 \rangle \quad F(\omega) = E_m \preceq \dots \preceq E_0 = K(\omega) \\ E_i \preceq E_{i-1} \text{ e' ciclica e di Galois, inoltre } \mathcal{G}(E_{i-1}, E_i) \simeq \frac{\Gamma_i}{\Gamma_{i-1}}$$

$$\left\{ \begin{array}{l} F(\omega) \preceq K(\omega) \text{ di Galois} \\ F(\omega) \preceq E_i \preceq K(\omega) \end{array} \right\} \xRightarrow{[6.23, \text{pg.96}]} E_i \preceq K(\omega) \text{ di Galois}$$

$$\left\{ \begin{array}{l} E_i \preceq K(\omega) \text{ di Galois} \\ \Gamma_{i-1} \preceq \Gamma_i \text{ normale} \\ \text{pezzo della catena risolvnte} \\ \Gamma_i \preceq \mathcal{G}(K(\omega), K(\omega)^{\Gamma_i}) = \mathcal{G}(K(\omega), E_i) \end{array} \right\} \xRightarrow{[6.31, \text{pg.105}]} E_i \preceq K(\omega)^{\Gamma_{i-1}} = E_{i-1} \text{ e' di Galois} \Rightarrow$$

$$\xRightarrow{[6.31, \text{pg.105}]} \mathcal{G}(K(\omega)^{\Gamma_{i-1}}, E_i) \simeq \frac{\mathcal{G}(K(\omega), E_i)}{\Gamma_{i-1}} = \frac{\Gamma_i}{\Gamma_{i-1}} \text{ che e' ciclico per la (3.2)}$$

$$\mathcal{G}(E_{i-1}, E_i) = \mathcal{G}(K(\omega)^{\Gamma_{i-1}}, E_i) \simeq \frac{\Gamma_i}{\Gamma_{i-1}} \text{ ciclico} \Rightarrow E_i \preceq E_{i-1} \text{ e' ciclica}$$

$$\langle 1.2 \rangle \quad [E_{i-1} : E_i] \Big/ n$$

$$E_i \preceq E_{i-1} \text{ di Galois} \Rightarrow [E_{i-1} : E_i] = |\mathcal{G}(E_{i-1}, E_i)| \xRightarrow{\text{passo 1.1}} \left| \frac{\Gamma_i}{\Gamma_{i-1}} \right| = p_i \Big/ \underbrace{n}_{(3.1)}$$

$\langle 1.3 \rangle$ Q.E.D.

$$\left\{ \begin{array}{l} \omega \in F(\omega) = E_m \preceq E_i \\ \text{ch} E_i = \text{ch} F = 0, \quad U_n = \langle \omega \rangle \\ E_i \preceq E_{i-1} \text{ e' ciclica e di Galois (passo 1.1)} \\ [E_{i-1} : E_i] \Big/ n \text{ (passo 1.2)} \end{array} \right\} \xRightarrow{[7.17, \text{pg.153}]} \exists b_i \in E_{i-1} : E_{i-1} = E_i(b_i), \quad b_i^n \in E_i$$

Quindi

$$F \preceq F(\omega) = E_m \preceq E_m(b_m) = E_{m-1} \preceq E_{m-1}(b_{m-1}) = E_{m-2} \preceq \dots \preceq E_1(b_1) = E_0 = K(\omega)$$

$$F \preceq F(\omega) \preceq F(\omega, b_m) \preceq F(\omega, b_m, b_{m-1}) \preceq \dots \preceq F(\omega, b_m, b_{m-1}, \dots, b_1) = E_0 = K(\omega)$$

$$\begin{cases} CS(f(x), F) = K \preceq K(\omega) = F(\omega, b_m, b_{m-1}, \dots, b_1) \\ b_i^n \in F(\omega, b_m, \dots, b_{i+1}) \quad \forall i = 1, \dots, m-1 \\ b_m^n \in F(\omega), \quad \omega^n = 1 \in F \end{cases} \quad \underbrace{\Rightarrow}_{\text{per def.}} f(x) \text{ e' risolubile per radicali}$$

(2) Dim $\Rightarrow$

Per il lemma [7.22,pg.158] si ha

$$\exists E : K = CS(f(x), F) \preceq E = F(\alpha_1, \dots, \alpha_m)$$

$$\forall i = 1, \dots, m \exists n_i : \alpha_i^{n_i} = b_i \in F_{i-1}$$

$$F_0 = F, \quad F_i = F_{i-1}(\alpha_i) \quad \forall i = 1, \dots, m$$

$$F \preceq E \text{ di Galois}$$

Sia $n = \text{mcm}\{n_1, \dots, n_m\}$, $U_n = \langle \omega \rangle$, si ha

$$\begin{cases} \text{ch} F = 0 \\ K = CS(f(x), F) \end{cases} \quad \underbrace{\Rightarrow}_{[6.22, \text{pg.96}]} F \preceq K \text{ e' di Galois} \quad \underbrace{\Rightarrow}_{[7.20, \text{pg.155}]} F(\omega) \preceq K(\omega) \text{ di Galois}$$

$$F \preceq E \text{ di Galois} \quad \underbrace{\Rightarrow}_{[7.20, \text{pg.155}]} F(\omega) \preceq E(\omega) \text{ di Galois}$$

$$\text{Sia } F' = F(\omega), \quad F'_i = F(\omega), \quad K' = K(\omega), \quad E' = E(\omega)$$

$$\begin{cases} F' \preceq K' \preceq E' \\ F' \preceq E' \text{ di Galois} \\ F' \preceq K' \text{ di Galois} \end{cases} \quad \underbrace{\Rightarrow}_{[6.30, \text{pg.101}]} \mathcal{G}(K', F') \simeq \frac{\mathcal{G}(E', F')}{\mathcal{G}(E', K')} \quad (1)$$

Inoltre, sempre per la prop [7.20,pg.155], si ha

$$\mathcal{G}(K, F) \text{ risolubile} \quad \underbrace{\Leftrightarrow}_{[7.20, \text{pg.155}]} \mathcal{G}(K', F') \text{ risolubile} \quad (2)$$

Per la (2) e poiche' vale la seguente implicazione:

$$\mathcal{G}(E', F') \text{ risolubile} \quad \underbrace{\Rightarrow}_{[7.3, \text{pg.140}]} \frac{\mathcal{G}(E', F')}{\mathcal{G}(E', K')} \simeq \mathcal{G}(K', F') \text{ risolubile}$$

basta dimostrare che $\mathcal{G}(E', F')$ e' risolubile .

(2.1) $\mathcal{G}(E', F')$ e' risolubile

$$\begin{aligned}
& \left\{ \begin{array}{l} F' \preceq F'_i \preceq E' \\ F' \preceq E' \text{ di Galois} \end{array} \right\} \xRightarrow{\text{[6.23,pg.96]}} F'_i \preceq E' \text{ di Galois} \\
& F'_{i+1} = F_{i+1}(\omega) = F_i(\omega, \alpha_{i+1}) = F'_i(\alpha_{i+1}) \\
& n_{i+1}/n = \text{mcm}\{n_1, \dots, n_m\} \Rightarrow U_{n_{i+1}} \subseteq U_n \xRightarrow{U_n = \langle \omega \rangle, \omega \in F_{i'}} F'_i \\
& \left\{ \begin{array}{l} F'_{i+1} = F'_i(\alpha_{i+1}) \\ \alpha_{i+1}^{n_{i+1}} \in F'_i \\ U_{n_{i+1}} \subseteq F'_i \\ \text{ch} F = 0 \end{array} \right\} \xRightarrow{\text{[7.17,pg.153]}} F'_i \preceq F'_{i+1} \text{ e' ciclica e di Galois} \quad (3) \\
& \Rightarrow \mathcal{G}(F'_{i+1}, F'_i) \text{ e' ciclico} \quad (3.1) \\
& \left\{ \begin{array}{l} F'_i \preceq E' \text{ di Galois} \\ F'_i \preceq F'_{i+1} \text{ di Galois} \end{array} \right\} \xRightarrow{\text{[6.30,pg.101]}} \frac{\mathcal{G}(E', F'_i)}{\mathcal{G}(E', F'_{i+1})} \simeq \mathcal{G}(F'_{i+1}, F'_i) \text{ ciclico per la (3.1), e quindi abeliano} \quad (3.2) \\
& \text{Applicando la corrispondenza di Galois (vedi [6.25,pg.96]) alla catena di campi} \\
& \quad F' \preceq F'_1 \preceq \dots \preceq F'_m = E' \\
& \text{otteniamo la catena di gruppi} \\
& \quad \{\text{id}\} \preceq \mathcal{G}(E', F_{m-1}) \preceq \dots \preceq \mathcal{G}(E', F') \\
& \text{che per la (3.2) e' una catena di gruppi che rende } \mathcal{G}(E', F') \text{ un gruppo risolubile.}
\end{aligned}$$

□

Lemma 7.24.

$$\begin{aligned}
& \forall p \geq 5 \text{ primo} \quad \exists f(x) \in \mathbb{Q}[x] \text{ irriducibile} : \deg f = p, \quad \begin{cases} \alpha_1, \dots, \alpha_{p-2} \in \mathbb{R} \\ \alpha_{p-1}, \alpha_p \in \mathbb{C} \setminus \mathbb{R} \end{cases} \\
& \text{dove } \alpha_1, \dots, \alpha_p \text{ sono le radici di } f
\end{aligned}$$

Proof: Siano $c, a_1, \dots, a_{p-2} \in 2\mathbb{Z}^*$ numeri pari non nulli, con $c \geq 2$, $a_1 < a_2 < \dots < a_{p-2}$ e tali che

$$\begin{aligned}
& \sum_{i=1}^{p-2} a_i = 0 \\
& c + \sum_{1 \leq i < j \leq p-2} a_i a_j > 0 \Leftrightarrow c > - \sum_{1 \leq i < j \leq p-2} a_i a_j
\end{aligned}$$

Siano dati i seguenti polinomi

$$\begin{aligned}
& g(x) = (x^2 + c)(x - a_1) \dots (x - a_{p-2}) \\
& f(x) = g(x) + 2 \\
& \deg f = \deg g = p
\end{aligned}$$

Sia A l'insieme delle radici di $f(x)$.

(1) $|A \cap \mathbb{R}| \geq p - 2$, ovvero, $f(x)$ ha almeno $p - 2$ radici reali

CASE: $g(a_i + 1) < 0$

$$\begin{aligned}
g(a_i + 1) &= ((a_i + 1)^2 + c) \prod_{j=1}^{p-2} (a_i + 1 - a_j) \\
c \geq 2 &\Rightarrow (a_i + 1)^2 + c \geq 2 \\
i = j &\Rightarrow |a_i + 1 - a_j| \geq 1 \\
i \neq j &\Rightarrow a_i < a_j \vee a_j < a_i \quad \underbrace{\Rightarrow}_{a_i, a_j \text{ pari}} \Rightarrow |a_i + 1 - a_j| \geq 1 \\
&\Rightarrow |g(a_i + 1)| \geq 2 \\
g(a_i + 1) < 0 &\Rightarrow g(a_i + 1) \leq -2 \quad (*) \\
f(a_i) = g(a_i) + 2 &\quad \underbrace{=}_{a_i \text{ e' radice di } g(x)} \quad 2 > 0 \\
f(a_i + 1) = g(a_i + 1) + 2 &\quad \underbrace{<}_{(*)} \leq 0
\end{aligned}$$

Se $f(a_i + 1) = 0$, allora $a_i + 1$ e' radice di f , altrimenti

$$f(a_i) > 0, \quad f(a_i + 1) < 0 \quad \underbrace{\Rightarrow}_{\text{thm esistenza degli zeri}} \quad \exists \xi_i \in \mathbb{R} : a_i < \xi < a_i + 1, \quad f(\xi_i) = 0$$

Quindi, in questo caso, per ogni radice a_i troviamo almeno una corrispondente radice di f .

Queste radici sono tutte distinte perche' ognuna appartiene a un intervallo del tipo $]a_i, a_{i+1}[$.

CASE: $g(a_i + 1) > 0$

Osservando che

$$\begin{aligned}
g(a_i + 1) &> 0 \\
g(a_i) &= 0 \\
g(a_{i+1}) &= 0 \\
a_{i-1} &< a_i - 1 < a_i < a_i + 1 < a_{i+1}
\end{aligned}$$

e studiando i punti di minimo e massimo relativo²⁶, si ricava che $g(a_i - 1) < 0$. A questo punto si procede analogamente al caso precedente.

(2) $f(x)$ e' irriducibile

$f(x)$ e' monico. Il suo termine noto non e' divisibile per 2^2 :

$$c \prod a_i + 2 = 2 \quad \mathbb{Z}_4$$

Allora per il criterio di Eisenstein, $f(x)$ e' irriducibile in $\mathbb{Q}[x]$.

(3) $|A \cap \mathbb{C} \setminus \mathbb{R}| = 2$

Supponiamo per assurdo che $A \subseteq \mathbb{R}$:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_p) \quad \alpha_i \in \mathbb{R} \quad \forall i$$

Applicando le formule di Viete' (vedi [4.7, pg. 72]) e ricordando che

$$f(x) = g(x) + 2 = (x^2 + c)(x - a_1) \dots (x - a_{p-2}) + 2$$

abbiamo:

1. Il coefficiente di x^{p-1} e'

$$\sum \alpha_i$$

²⁶ $g(x)$ ha tutte le radici distinte, quindi a_i non puo' essere una radice di $g'(x)$ e quindi $g'(a_i)$ non puo' essere ne' un punto di minimo ne' di massimo

ma e' anche

$$-\sum a_i \underbrace{=}_{\text{per Hp}} = 0$$

quindi

$$\sum \alpha_i = 0$$

2. Il coefficiente di x^{p-2} e'

$$c + \sum_{1 \leq i < j \leq p-2} a_i a_j > 0 \quad (*)$$

ma e' anche

$$\sum_{1 \leq h < l \leq p} \alpha_h \alpha_l \underbrace{=}_{\text{ragionando sui doppi prodotti}} \frac{1}{2} \left(\left(\sum \alpha_h \right)^2 - \sum \alpha_h^2 \right) \underbrace{=}_{\sum \alpha_i = 0} -\frac{1}{2} \sum \alpha_h^2 \underbrace{\leq}_{\alpha_h \in \mathbb{R}} 0$$

che e' assurdo contro (*).

Quindi,

$$A \not\subseteq \mathbb{R} \Rightarrow \exists \alpha \in \mathcal{A}^{\mathbb{C}} : f(\alpha) = 0, f(\bar{\alpha}) = 0$$

$\bar{\alpha}$ coniugata di α

Quindi $f(x)$ ha almeno due radici complesse.

$$\begin{cases} \deg f = p \Rightarrow |A| \leq p \\ |A \cap \mathbb{R}| \geq p-2 \\ |A \cap \mathbb{C} \setminus \mathbb{R}| \geq 2 \end{cases} \Rightarrow |A \cap \mathbb{C} \setminus \mathbb{R}| = 2$$

Ovvero, $f(x)$ ha solo due radici complesse. □

Proposition 7.25.

$$\forall p \geq 5 \text{ primo } \exists f(x) \text{ irrid. in } \mathbb{Q}[x] \text{ t.c. } \mathcal{G}(L, \mathbb{Q}) \simeq S_p(A)$$

dove $L = CS(f(x), \mathbb{Q})$, A e' l'insieme delle radici di $f(x)$

Proof: Per il lemma [7.24,pg.163] esiste $f(x) \in \mathbb{Q}[x]$ irriducibile, con due sole radici complesse, con $\deg f = p$.

Sia $L = CS(f(x), \mathbb{Q})$.

$$\text{ch}\mathbb{Q} = 0 \Rightarrow \mathbb{Q} \preceq L \text{ separabile} \underbrace{\Rightarrow}_{f(x) \text{ irrid.}} f(x) \text{ separabile} \Rightarrow \mathbb{Q} \preceq L \text{ di Galois (1)}$$

$$f(x) \text{ irrid.} \Rightarrow \deg f = p \Big/ [L : \mathbb{Q}] \underbrace{=}_{(1)} |\mathcal{G}(L, \mathbb{Q})| \underbrace{\Rightarrow}_{\text{thm Cauchy [AII,1.177,pg.75]}} \exists g \in \mathcal{G}(L, \mathbb{Q}) : o(g) = p$$

Sia $A = \{\alpha_1, \dots, \alpha_p\}$ l'insieme delle radici di $f(x)$, dove α_1, α_2 sono le due radici complesse (coniugate tra loro). Per la prop [6.26,pg.99] abbiamo

$$\mathcal{G}(L, \mathbb{Q}) \leq S_p(A)$$

²⁷ g e' un p -ciclo di $S_p(A)$, infatti,

$$g = \gamma_1 \dots \gamma_r, \quad \gamma_1, \dots, \gamma_r \text{ cicli disgiunti}$$

$$o(g) = p = \text{mcm} \{l(\gamma_i) \mid i = 1, \dots, r\} \underbrace{\Rightarrow}_{p \text{ primo}} \exists! i : l(\gamma_i) = p, \text{ tutte le altre sono di lunghezza } 1$$

$$\Rightarrow g = \gamma_i \Rightarrow l(g) = p$$

²⁷stiamo pensando $\mathcal{G}(L, \mathbb{Q})$ come un vero sottogruppo di $S_p(A)$, in realta' e' solo immerso in $S_p(A)$. La dimostrazione pero' rimane invariata.

Sia τ' la coniugazione complessa e sia $\tau = \tau'|_L$. Si ha

$$\begin{cases} \tau \in \mathcal{I}(L, \mathbb{Q}) = \mathcal{G}(L, \mathbb{Q}) \\ \tau(\alpha_1) = \alpha_2, \quad \tau(\alpha_i) \underbrace{=}_{\alpha_i \in \mathbb{R}} \alpha_i \quad \forall i > 2 \quad \Rightarrow \tau = (\alpha_1, \alpha_2) \text{ trasposizione} \end{cases}$$

g p -ciclo di $S_p(A) \Rightarrow g$ muove tutti gli elementi di $A \Rightarrow g = (\dots, \alpha_1, \dots, \alpha_2, \dots) \Rightarrow \exists i : g^i(\alpha_1) = \alpha_2$

$$o(g^i) = \frac{o(g)}{\text{MCD}(o(g), i)} = \frac{p}{(p, i)} = 1, p, \quad g^i \neq \text{id} \Rightarrow g^i \text{ e' un } p\text{-ciclo}$$

Sia $g' = g^i \in \mathcal{G}(L, \mathbb{Q})$

A meno di rinominare gli indici di $\alpha_3, \dots, \alpha_r$, possiamo scrivere

$$g' = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_r) \in \mathcal{G}(L, \mathbb{Q})$$

Infine, abbiamo

$$\begin{cases} \tau = (\alpha_1, \alpha_2), \quad g' = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_p) \in \mathcal{G}(L, \mathbb{Q}) \\ S_p(A) \underbrace{=}_{[\text{AII}, 1.85, \text{pg.} 32]} \langle \tau, g' \rangle \quad \Rightarrow S_p(A) \subseteq \mathcal{G}(L, \mathbb{Q}) \subseteq S_p(A) \Rightarrow S_p(A) = \mathcal{G}(L, \mathbb{Q}) \end{cases}$$

□

Theorem 7.26.

$\forall p \geq 5 \exists f(x) \in \mathbb{Q}[x]$ irriducibile, $\deg f = p$ t.c. $f(x)$ non e' risolubile per radicali

Con questo teorema possiamo quindi affermare che non esistono formule che risolvono qualsiasi polinomio di grado ≥ 5 e che facciano uso delle operazioni $+$, $-$, $*$, $/$, $\sqrt{}$.

Proof: Basta applicare la prop [7.25,pg.165], il thm [7.7,pg.146] e il thm [7.23,pg.160]. (nota 28) □

7.4 Discriminante

Definition 7.27. Sia F campo, $\bar{x} = (x_1, \dots, x_n)$ indeterminate, con $n \geq 2$. Definiamo il discriminante:

$$\Delta(\bar{x}) \stackrel{\text{def}}{=} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in F[\bar{x}]$$

e poniamo

$$\sqrt{\Delta}(\bar{x}) \stackrel{\text{def}}{=} \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Proposition 7.28.

1. $\Delta(\bar{x})$ e' simmetrico
2. $\sigma \in S_n \Rightarrow \sqrt{\Delta}(\sigma(\bar{x})) = \text{sgn}(\sigma) \sqrt{\Delta}(\bar{x})$

$$\text{dove } \sigma(\bar{x}) = (x_{\sigma(1)}, \dots, x_{\sigma(n)}), \quad \text{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ pari} \\ -1 & \sigma \text{ dispari} \end{cases}$$

28

$$K = CS(f(x), \mathbb{Q})$$

$$\text{ch}\mathbb{Q} = 0, \quad \mathbb{Q} \preceq K \text{ algebrica} \quad \underbrace{\Rightarrow}_{[3.23, \text{pg.} 60]} \quad \mathbb{Q} \preceq K \text{ separabile} \quad \underbrace{\Rightarrow}_{f(x) \in \mathbb{Q}[x] \text{ irriducibile}} \quad \Rightarrow f(x) \text{ separabile}$$

Essendo $\Delta(\bar{x})$ simmetrico, per il thm [4.8,pg.73], si ha

$$\exists! \Delta_{sym} \in F[\bar{x}] : \Delta(\bar{x}) = \Delta_{sym}(\sigma_1(\bar{x}), \sigma_2(\bar{x}), \dots, \sigma_n(\bar{x}))$$

Proof:

(1) Dim 1.

$$\Delta(\bar{x}) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = \prod_{1 \leq i < j \leq n} -(x_i - x_j)(x_j - x_i) = (-1)^N \prod_{1 \leq i < j \leq n} (x_i - x_j)(x_j - x_i)$$

dove $N = |\{\{i, j\} \mid 1 \leq i < j \leq n\}|$

Poiche' l'insieme $\{\{i, j\} \mid 1 \leq i < j \leq n\}$ contiene tutti i possibili raggruppamenti, a due a due, di $\{1, 2, \dots, n\}$, abbiamo che

$$N = \binom{n}{2}$$

quindi, si vede facilmente che

$$\Delta(\bar{x}) = (-1)^{\binom{n}{2}} \prod_{i \neq j} (x_i - x_j)$$

e da qui si capisce che $\Delta(\bar{x})$ e' simmetrico.

(2) Dim 2.

Poiche' ogni $\sigma \in S_n$ e' prodotto di trasposizioni, basta dimostrare che

$$\sqrt{\Delta}(\tau(\bar{x})) = -\sqrt{\Delta}(\bar{x}) \quad \forall \tau \text{ trasposizione di } S_n$$

Sia $\tau = (i, j)$, con $i < j$, si ha

$$\sqrt{\Delta}(\bar{x}) = \prod_{1 \leq h < k \leq n} (x_h - x_k) =$$

$$= (x_i - x_j) \prod_{1 \leq h < k \leq n, (h,k) \neq (i,j)} (x_h - x_k) = \pm (x_i - x_j) \prod_{m \neq i, m \neq j} (x_i - x_m)(x_j - x_m) \prod_{h < k, h \neq i, j, k \neq i, j} (x_h - x_k)$$

$$\sqrt{\Delta}(\tau(\bar{x})) = \pm (x_j - x_i) \prod_{m \neq i, m \neq j} (x_j - x_m)(x_i - x_m) \prod_{h < k, h \neq i, j, k \neq i, j} (x_h - x_k) = -\sqrt{\Delta}(\bar{x})$$

□

Example 7.29.

$$n = 2 \Rightarrow \Delta(\bar{x}) = (x_1 - x_2)^2 = \sigma_1^2 - 4\sigma_2$$

dove $\sigma_1, \sigma_2 \in F[x_1, x_2]$ sono i polinomi simmetrici elementari.

Proof:

$$\Delta(\bar{x}) = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2$$

□

Definition 7.30. Sia dato il polinomio monico

$$f(x) = x^n + a_1x^{n-1} + \dots + a_n \in F[x]$$

Se $n \geq 2$, definiamo il :

$$\delta(f) = \Delta_{sym}(-a_1, \dots, (-1)^i a_i, \dots, (-1)^n a_n) \in F$$

dove $\Delta(\bar{x}) \in F[\bar{x}]$, e $\Delta_{sym}(\bar{x})$ e' dato dalla prop [7.28,pg.166].

Per $n \leq 1$, poniamo $\delta(f) = 1$.

Infine, con $\sqrt{\delta(f)}$ indichiamo una qualsiasi radice di $x^2 - \delta(f)$.

Example 7.31. Continuiamo l'esempio [7.29,pg.167]. Per $n = 2$ si ha

$$\begin{aligned}\Delta_{\text{sym}}(\sigma_1, \sigma_2) &= \sigma_1^2 - 4\sigma_2 \\ \delta(x^2 + bx + c) &= \Delta_{\text{sym}}(-b, c) = b^2 - 4c\end{aligned}$$

Proposition 7.32. Sia $\alpha = (\alpha_1, \dots, \alpha_n)$ il vettore delle radici del polinomio monico $f(x) \in F[x]$. Si ha

1. $\delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \Delta(\alpha)$
- 1.1 $\sqrt{\delta(f)} = \pm \sqrt{\Delta(\alpha)}$
2. $\delta(f) \in F, \sqrt{\delta(f)} \in L = CS(f(x), F)$
3. $f(x)$ separabile $\Leftrightarrow \delta(f) \neq 0$

Proof: Sia $f(x) = x^n + a_1x^{n-1} + \dots + a_n$, si ha

$$\Delta(\alpha) = \Delta_{\text{sym}}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \underset{\substack{= \\ \text{formule di Viete' [4.7,pg.72]}}}{=} \Delta_{\text{sym}}(-a_1, \dots, (-1)^n a_n) = \delta(f)$$

Dalla definizione segue subito che $\delta(f) \in F$. Per quanto riguarda $\sqrt{\delta(f)}$:

$$\begin{aligned}\alpha_i \in L \quad \forall i &\Rightarrow \sqrt{\delta(f)} = \pm \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in L \\ \sqrt{\delta(f)} &= \pm \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) = \pm \sqrt{\Delta(\alpha)}\end{aligned}$$

Infine, la 3. segue direttamente dalla 1. □

Proposition 7.33. Sia $f(x) \in F[x]$ separabile e monico, $\deg f = n$, $L = CS(f(x), F)$.

1. $\varphi \in \mathcal{G}(L, F) \Rightarrow \varphi(\sqrt{\delta(f)}) = \text{sgn}(\varphi') \sqrt{\delta(f)}$
dove φ' e' l'immagine di φ tramite l'immersione $G = \mathcal{G}(L, F) \hookrightarrow S_n$, ovvero $G \simeq G' \leq S_n$
2. Se $\text{ch} F \neq 2$ si ha
 $G' \leq A_n \Leftrightarrow \sqrt{\delta(f)} \in F$

Proof:

(1) Dim 1.

Per la prop [7.32,pg.168] si ha

$$\sqrt{\delta(f)} = \pm \sqrt{\Delta(\alpha)}$$

supponiamo dapprima che $\sqrt{\delta(f)} = +\sqrt{\Delta(\alpha)}$.

Sia $\alpha = (\alpha_1, \dots, \alpha_n)$ il vettore delle radici di f .

$$\sqrt{\Delta(\varphi'(\bar{x}))} \underset{=}{=} \text{sgn}(\varphi') \sqrt{\Delta(\bar{x})} \quad (1)$$

[7.28,pg.166]

$$\varphi(\sqrt{\delta(f)}) = \varphi(\sqrt{\Delta(\alpha)}) \underset{\substack{= \\ \varphi \text{ permuta le } \alpha_i}}{=} \sqrt{\Delta(\varphi'(\alpha))} \underset{(1)}{=} \text{sgn}(\varphi') \sqrt{\Delta(\alpha)} \underset{=}{=} \text{sgn}(\varphi') \sqrt{\delta(f)} \quad [7.32,pg.168]$$

Si procede in modo analogo nel caso $\sqrt{\delta(f)} = -\sqrt{\Delta(\alpha)}$.

(2) Dim 2.

$$f(x) \text{ separabile}, L = CS(f(x), F) \xRightarrow{[6.19, \text{pg.92}]} F \preceq L \text{ di Galois} \Rightarrow L^{\mathcal{G}(L, F)} = F$$

$$\varphi(\sqrt{\delta(f)}) \underset{1.}{=} \text{sgn}(\varphi') \sqrt{\delta(f)} \quad (2)$$

$$G' \leq A_n \Leftrightarrow \varphi' \in A_n \quad \forall \varphi' \in G' \Leftrightarrow \text{sgn}(\varphi') = 1 \quad \forall \varphi' \in G' \xRightarrow{(2), (*)}$$

$$\Leftrightarrow \varphi(\sqrt{\delta(f)}) = \sqrt{\delta(f)} \quad \forall \varphi \in G \Leftrightarrow \sqrt{\delta(f)} \in L^{\mathcal{G}(L, F)} = F$$

(*) NOTA: nell'implicazione $\Leftarrow$ stiamo implicitamente sfruttando l'ipotesi $\text{ch}F \neq 2$, infatti, solo in $\text{ch}F = 2$ si ha

$$1 + 1 = 0 \Rightarrow 1 = -1$$

$$\sqrt{\delta(f)} = \text{sgn}(\varphi') \sqrt{\delta(f)} \xRightarrow{f \text{ separabile} \Rightarrow \delta(f) \neq 0} \text{sgn}(\varphi') = 1 = -1$$

Quindi in $\text{ch}F = 2$ non sappiamo distinguere il segno di φ' .

□

Proposition 7.34. Sia $f(x) \in F[x]$ monico, irriducibile, separabile²⁹, $\deg f = 3$, $L = CS(f(x), F)$, $\text{ch}F \neq 2$.

Si ha

$$\mathcal{G}(L, F) \simeq \begin{cases} A_3 \Leftrightarrow \sqrt{\delta(f)} \in F \\ S_3 \Leftrightarrow \sqrt{\delta(f)} \notin F \end{cases}$$

Proof: Sia α una radice di $f(x)$,

$$f(x) \text{ separabile}, L = CS(f(x), F) \xRightarrow{[6.19, \text{pg.92}]} F \preceq L \text{ di Galois} \Rightarrow [L : F] = |\mathcal{G}(L, F)|$$

$$f(x) \text{ irriducibile} \Rightarrow [F(\alpha) : F] = 3 \xRightarrow{F \preceq F(\alpha) \preceq L} 3 \Big/ [L : F] = |\mathcal{G}(L, F)| \xRightarrow{[6.27, \text{pg.100}]} |S_3| = 3! = 6$$

$$\Rightarrow |\mathcal{G}(L, F)| = 3, 6 \Leftrightarrow \mathcal{G}(L, F) \simeq A_3, S_3$$

$$\mathcal{G}(L, F) \simeq A_3 \xRightarrow{[7.33, \text{pg.168}]} \sqrt{\delta(f)} \in F$$

$$\mathcal{G}(L, F) \simeq S_3 \xRightarrow{A_3 < S_3} \mathcal{G}(L, F) \not\hookrightarrow A_3 \xRightarrow{[7.33, \text{pg.168}]} \sqrt{\delta(f)} \notin F$$

□

²⁹per la prop [7.32, pg.168],

$$f \text{ separabile} \Leftrightarrow \delta(f) \neq 0$$

8 Esercizi

Example 8.1. 1. $\sqrt{2} + \sqrt{3}$ e' algebrico su $\mathbb{Q}$, e $P_{\min}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$

2. $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = 4$ e una base e' $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Proof:

(1) Dim 1.

$\sqrt{2}, \sqrt{3}$ sono algebrici su $\mathbb{Q}$, infatti, basta considerare

$$x^2 - 2, \quad x^2 - 3$$

Allora, per la [2.46,pg.33], si ha che $\sqrt{2} + \sqrt{3}$ e' algebrico su $\mathbb{Q}$.

$$f(x) = x^4 - 10x^2 + 1 =$$

$$= (x - (\sqrt{2} + \sqrt{3}))(x + (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x + (\sqrt{2} - \sqrt{3})) = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6}) \quad (*)$$

$f(x)$ e' monico, e $f(\sqrt{2} + \sqrt{3}) = 0$. $f(x)$ e' irriducibile, infatti, se per assurdo

$$f(x) = p(x)q(x), \quad p(x), q(x) \in \mathbb{Q}[x], \quad p(x), q(x) \text{ irriducibili}$$

$$\deg f(x) = \deg p(x)q(x) = \deg p(x) + \deg q(x)$$

si ha

$$\text{CASE: } \deg p(x) = 2$$

$$\deg q(x) = 2$$

Quindi $f(x)$ e' fattorizzato in polinomi irriducibili di grado 2. Allora, per la (*), e poiche'

$\mathbb{Q}[x]$ e' un UFD, $f(x)$ e' del tipo

$$f(x) = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6})$$

ma in questo modo, $f(x) \notin \mathbb{Q}[x]$. Assurdo.

$$\text{CASE: } \deg p(x) = 1$$

$$p(x) = x - \alpha \mid f(x)$$

Sempre per la (*), e poiche' $\mathbb{Q}[x]$ e' un UFD, si ha che $x - \alpha$ deve essere uguale a uno dei fattori lineari visti in (*). Assurdo contro $p(x) \in \mathbb{Q}[x]$.

$$\text{CASE: } \deg p(x) = 3$$

$$\deg q(x) = 1$$

quindi basta applicare il caso precedente.

Abbiamo cosi' visto che $f(x)$ e' monico, $f(\sqrt{2} + \sqrt{3}) = 0$ e $f(x)$ e' irriducibile in $\mathbb{Q}[x]$. Allora per la [2.30,pg.24], si ha

$$f(x) = P_{\min}(\sqrt{2} + \sqrt{3}, \mathbb{Q})$$

(2) Dim 2.

Consideriamo la seguente catena:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \quad (3)$$

Si ha

$$x^2 - 2 \begin{cases} \text{monico} \\ \text{irriducibile in } \mathbb{Q}[x] \\ \text{ha } \sqrt{2} \text{ come radice} \end{cases} \xRightarrow{[2.30, \text{pg.24}]} P_{\min}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \Rightarrow$$

$$\xRightarrow{[2.40, \text{pg.29}]} \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \deg(x^2 - 2) = 2, \quad B = \{1, \sqrt{2}\} \text{ e' una base}$$

Analogamente, poiche' $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ e' irriducibile in $\mathbb{Q}(\sqrt{2})[x]$, si ha
 $P_{\min}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3 \Rightarrow \dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \deg(x^2 - 3) = 2$

$C = \{1, \sqrt{3}\}$ e' una base

Allora

$$(3) \xRightarrow{[2.18, \text{pg.16}]} \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = 4, \quad BC = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \text{ e' una base}$$

(3) Dim 3.

Consideriamo la seguente catena:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Si ha

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + \sqrt{3}) \xRightarrow{[2.40, \text{pg.29}]} \deg P_{\min}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) \xRightarrow{1} \deg(x^4 - 10x^2 + 1) = 4$$

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \xRightarrow{2} = 4$$

$$\begin{cases} \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \text{sottospazio vettoriale} \\ \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \end{cases} \xRightarrow{[AL, 4.10.2, \text{pg.27}]} \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

□

Example 8.2.

1. Calcolare $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}^{\frac{1}{4}}, \sqrt{3}^{\frac{1}{3}})$.
2. Calcolare $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + \sqrt{2})$ e trovare una sua base.

Proof:

(1) Dim 1.

Consideriamo le due catene:

$$\mathbb{Q} \subseteq \mathbb{Q}(2^{\frac{1}{4}}) \subseteq \mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}})$$

$$\mathbb{Q} \subseteq \mathbb{Q}(3^{\frac{1}{3}}) \subseteq \mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}})$$

Per la transitivita' dei gradi (vedi [2.18, pg.16]), si ha

$$[\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{4}})] [\mathbb{Q}(2^{\frac{1}{4}}) : \mathbb{Q}] \quad (1)$$

$$[\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}(3^{\frac{1}{3}})] [\mathbb{Q}(3^{\frac{1}{3}}) : \mathbb{Q}]$$

Si ha

$$P_{\min}(2^{\frac{1}{4}}, \mathbb{Q}) = x^4 - 2 \Rightarrow [\mathbb{Q}(2^{\frac{1}{4}}) : \mathbb{Q}] = 4$$

$$P_{\min}(3^{\frac{1}{3}}, \mathbb{Q}) = x^3 - 3 \Rightarrow [\mathbb{Q}(3^{\frac{1}{3}}) : \mathbb{Q}] = 3$$

Allora, sostituendo nella (1), abbiamo

$$\begin{cases} 4 / [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] \\ 3 / [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] \end{cases} \Rightarrow \text{mcm}(4, 3) = 12 / [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] \Rightarrow 12 \leq [\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}]$$

Ma per la prop. [2.42,pg.30], si ha

$$[\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] \leq [\mathbb{Q}(2^{\frac{1}{4}}) : \mathbb{Q}][\mathbb{Q}(3^{\frac{1}{3}}) : \mathbb{Q}] = 12$$

Quindi $[\mathbb{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{3}}) : \mathbb{Q}] = 12$

(2) Dim 2.

$$(2.1) \quad \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \text{ ovvero } \mathbb{Q}(\sqrt{2}, \sqrt{2 + \sqrt{2}}) = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$$

$$\sqrt{2} = (\sqrt{2} + 2) - 2 = \left(\sqrt{2 + \sqrt{2}} \right)^2 - 2 \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2 + \sqrt{2}}) \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2 + \sqrt{2}})$$

Possiamo così considerare la seguente catena:

$$\mathbb{Q} \preceq \mathbb{Q}(\sqrt{2}) \preceq \mathbb{Q}(\sqrt{2}, \sqrt{2 + \sqrt{2}}) = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$$

$$(2.2) \quad P_{\min} \left(\sqrt{2 + \sqrt{2}}, \mathbb{Q}(\sqrt{2}) \right) = x^2 - (2 + \sqrt{2})$$

$\sqrt{2 + \sqrt{2}}$ e' una radice di $x^2 - (2 + \sqrt{2})$

$x^2 - (2 + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$, ed e' monico

$x^2 - (2 + \sqrt{2})$ e' irrid. in $\mathbb{Q}(\sqrt{2})$, infatti, se non lo fosse:

$$x^2 - (2 + \sqrt{2}) = (x - \alpha)(x - \beta), \quad \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \quad (*)$$

$$x^2 - (2 + \sqrt{2}) = \left(x - \sqrt{2 + \sqrt{2}} \right) \left(x + \sqrt{2 + \sqrt{2}} \right) \Rightarrow \underbrace{\sqrt{2 + \sqrt{2}} = \alpha \in \mathbb{Q}(\sqrt{2})}_{(*), \text{ UFD}}$$

$$\begin{cases} [1, \sqrt{2}] \text{ e' una base di } \mathbb{Q}(\sqrt{2}) \\ \sqrt{2 + \sqrt{2}} \in \mathbb{Q}(\sqrt{2}) \end{cases} \Rightarrow \sqrt{2 + \sqrt{2}} = a + b\sqrt{2}, \quad a, b \in \mathbb{Q} \Rightarrow 2 + \sqrt{2} = a^2 + 2b^2 + 2\sqrt{2}ab \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a^2 + 2b^2 = 2 \\ 2ab = \sqrt{2} \end{cases} \Rightarrow \sqrt{2} = 2ab \in \mathbb{Q} \quad \text{assurdo}$$

Quindi per la prop [2.30,pg.24] si ha

$$P_{\min} \left(\sqrt{2 + \sqrt{2}}, \mathbb{Q}(\sqrt{2}) \right) = x^2 - (2 + \sqrt{2})$$

$$P_{\min} \left(\sqrt{2}, \mathbb{Q} \right) = x^2 - 2 \Rightarrow [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

$$P_{\min} \left(\sqrt{2 + \sqrt{2}}, \mathbb{Q}(\sqrt{2}) \right) = x^2 - (2 + \sqrt{2}) \Rightarrow [\mathbb{Q}(\sqrt{2}, \sqrt{2 + \sqrt{2}}) : \mathbb{Q}(\sqrt{2})] = 2$$

$$\underbrace{\Rightarrow}_{[2.18, \text{pg.16}]} [\mathbb{Q}(\sqrt{2}, \sqrt{2 + \sqrt{2}}) : \mathbb{Q}] = 4 \quad \underbrace{\Leftrightarrow}_{\text{passo 2.1}} [\mathbb{Q}(\sqrt{2 + \sqrt{2}}) : \mathbb{Q}] = 4$$

Trovare la base e' ora semplice. Conosciamo gia' le dimensioni di $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$, basta quindi applicare la prop [2.40,pg.29]:

$$\left\{ 1, \sqrt{2 + \sqrt{2}}, \left(\sqrt{2 + \sqrt{2}} \right)^2, \left(\sqrt{2 + \sqrt{2}} \right)^3 \right\} \text{ e' una base di } \mathbb{Q}(\sqrt{2 + \sqrt{2}})$$

Alternativamente potevamo calcolare una base di $\mathbb{Q} \preceq \mathbb{Q}(\sqrt{2})$, una di $\mathbb{Q}(\sqrt{2}) \preceq \mathbb{Q}(\sqrt{2 + \sqrt{2}})$ e farne il prodotto utilizzando la prop. [2.18,pg.16].

□

Example 8.3. 1. Trovare $K = CS(x^3 - 2, \mathbb{Q})$, e $\dim_{\mathbb{Q}} K$

Proof: Considerando l'estensione $\mathbb{Q} \preceq \mathbb{C}$, per la prop [1.19,pg.7], tutte le radici di $x^3 - 2$ sono $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

Quindi, per definizione,

$$CS(x^3 - 2, \mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$$

(1) Dim. che $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

Chiamiamo A e B i due insiemi.

(1.1) $\text{Dim} \subseteq$

Si ha $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \in A$, e quindi per definizione³⁰ $A \subseteq B$

(1.2) $\text{Dim} \supseteq$

Poiche' $\sqrt[3]{2} \in A$, Basta far vedere che $\omega \in A$:

$$\omega = \frac{\sqrt[3]{2}\omega^2}{\sqrt[3]{2}} \in A$$

Quindi, per definizione $B \subseteq A$

(2) Possiamo adesso calcolare $\dim_{\mathbb{Q}} K$ piu' agevolmente: basta calcolare $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, \omega)$

(2.1) $P_{\min}(\omega, \mathbb{Q}(\sqrt[3]{2})) = x^2 + x + 1$

ω e' radice di $x^3 - 1 \Leftrightarrow \omega$ e' radice di $(x - 1)(x^2 + 1 + x) \xRightarrow[\omega \neq 1]{} \omega$ e' radice di $x^2 + 1 + x$

$x^2 + 1 + x$ e' monico

Se per ass. $x^2 + 1 + x$ fosse riducibile in $\mathbb{Q}(\sqrt[3]{2})$: $x^2 + x + 1 = (x - \alpha)(x - \beta) \in \mathbb{Q}(\sqrt[3]{2})[x] \Rightarrow \alpha, \beta \in \mathbb{Q}(\sqrt[3]{2})$ (*)

Ma $x^2 + x + 1 = \left(x - \frac{-1 + i\sqrt{3}}{2}\right) \left(x - \frac{-1 - i\sqrt{3}}{2}\right) \xRightarrow{(*), \text{UFD}} \frac{-1 + i\sqrt{3}}{2} = \alpha \in \mathbb{Q}(\sqrt[3]{2})$ assurdo

Quindi per la prop [2.30,pg.24],

$$P_{\min}(\omega, \mathbb{Q}(\sqrt[3]{2})) = x^2 + x + 1$$

Abbiamo:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$P_{\min}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2 \xRightarrow{[2.40, \text{pg.29}]} [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$P_{\min}(\omega, \mathbb{Q}(\sqrt[3]{2})) = x^2 + x + 1 \xRightarrow{[2.40, \text{pg.29}]} [\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}(\sqrt[3]{2})] = 2 \xLeftrightarrow{[2.22, \text{pg.19}]} [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$$

$$\xRightarrow{[2.18, \text{pg.16}]} [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$$

□

Example 8.4.

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3}) \quad \forall \lambda \in \mathbb{Q}^*$$

³⁰ $F(\alpha_1, \alpha_2)$ e' il piu' piccolo sottocampo contenente F, α_1, α_2

Proof:

$\sqrt{2}, \sqrt{3}$ sono radici di $x^2 - 2, x^2 - 3 \in \mathbb{Q}[x] \Rightarrow \sqrt{2}, \sqrt{3}$ algebrici su $\mathbb{Q} \xRightarrow{[2.43, \text{pg.31}]} \mathbb{Q} \preceq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ algebrica

$$\begin{cases} \text{ch}\mathbb{Q} = 0 \\ \mathbb{Q} \preceq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \text{ algebrica} \end{cases} \xRightarrow{[3.23, \text{pg.60}]} \mathbb{Q} \preceq \mathbb{Q}(2, \sqrt{3}) \text{ separabile}$$

Allora applicando il thm [3.29, pg.65], abbiamo

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \lambda\sqrt{3}) \quad \forall \lambda \in \mathbb{Q} : \lambda \neq \frac{\alpha - \alpha_i}{\beta_2 - \beta} \quad \forall i = 1, 2$$

$$\text{dove } P_{\min}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \Rightarrow \alpha = \alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}$$

$$P_{\min}(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \Rightarrow \beta = \beta_1 = \sqrt{3}, \beta_2 = -\sqrt{3}$$

$$\lambda \neq 0 \wedge \lambda \neq \frac{2\sqrt{2}}{-2\sqrt{3}} = \frac{\sqrt{2}}{\sqrt{3}}$$

Poiche' $\frac{\sqrt{2}}{\sqrt{3}} \notin \mathbb{Q}$, mentre $\lambda \in \mathbb{Q}$, basta imporre che

$$\lambda \in \mathbb{Q}^*$$

□

Example 8.5. Trovare un campo con 8 elementi.

Proof: Dato che $8 = 2^3$, cerchiamo di usare la prop [3.6, pg.52]. Cerchiamo quindi un $f(x) \in \mathbb{Z}_2[x]$ irriducibile di grado 3. Poiche' i coefficienti di $f(x)$ possono essere 0 o 1, abbiamo solo 4 possibilita'. Tra questi polinomi prendiamo quello che non ha radici. Quindi,

$$\frac{\mathbb{Z}_2[x]}{(x^3 + x^2 + 1)} \text{ e' il campo cercato, infatti,}$$

$$x^3 + x^2 + 1 \text{ non ha radici: } 0^3 + 0^2 + 1 = 1, \quad 1^3 + 1^2 + 1 = 3 = 1$$

$$\deg x^3 + x^2 + 1 = 3$$

$$\Rightarrow x^3 + x^2 + 1 \text{ e' irriducibile}$$

allora per la prop [3.6, pg.52], si ha la tesi

□

Example 8.6. Sia $f(x) = x^4 + 1$, si ha

$$1. \quad CS(f(x), \mathbb{Q}) = \mathbb{Q}(\sqrt{2}, \sqrt{2}i)$$

$$2. \quad CS(f(x), \mathbb{R}) = \mathbb{R}(i)$$

Proof:

$$x^4 + 1 = (x^2 - i)(x^2 + i) = (x - \frac{\sqrt{2}}{2}(1 + i))(x + \frac{\sqrt{2}}{2}(1 + i))(x - \frac{\sqrt{2}}{2}(i - 1))(x + \frac{\sqrt{2}}{2}(i - 1))$$

$$CS(f(x), \mathbb{Q}) = \mathbb{Q}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}i - \frac{\sqrt{2}}{2}) = \mathbb{Q}(\sqrt{2}(1 + i), \sqrt{2}(i - 1)) \xRightarrow{(*)} \mathbb{Q}(\sqrt{2}, \sqrt{2}i)$$

$$(*) \quad \frac{\sqrt{2}(1 + i) - \sqrt{2}(i - 1)}{2} = \sqrt{2}, \quad \frac{\sqrt{2}(1 + i) + \sqrt{2}(i - 1)}{2} = \sqrt{2}i$$

$$CS(f(x), \mathbb{R}) = \mathbb{R}(\sqrt{2}, \sqrt{2}i) = \mathbb{R}(i)$$

□

Example 8.7. $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ e' una estensione normale ma non finita.

Proof:

(1) Dim. che $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ e' non finita

(1.1) Metodo 1

Se per assurdo $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ fosse finita, allora

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = n \quad (1)$$

$$\overline{\mathbb{Q}} = \underbrace{\{\alpha \in \mathbb{C} \mid \alpha \text{ algebrico su } \mathbb{Q}\}}_{[2.64, \text{pg.50}]} \Rightarrow \{\sqrt{p} \mid p \in \mathbb{Z} \text{ primo}\} \subseteq \overline{\mathbb{Q}} \quad (2)$$

Sia p_i l' i -esimo primo

(1), (2) $\Rightarrow \sqrt{p_1}, \dots, \sqrt{p_m}$, con $m > n$, sono l.d., quindi

$$\exists i \leq m : \sqrt{p_i} = a_1\sqrt{p_1} + a_2\sqrt{p_2} + \dots + a_h\sqrt{p_h}, \quad 1 \leq h < i, \quad a_i \in \mathbb{Q} \quad \forall i = 1, \dots, h$$

Se $h = 1$, allora

$$\sqrt{p_i} = a_1\sqrt{p_1} \Rightarrow p_i = a_1^2 p_1 \Rightarrow \underbrace{a_1}_{p_i \text{ primo}} = 1, \quad p_i = p_1$$

assurdo contro $i > 1$. Se $h \geq 2$,

$$p_i = (a_1\sqrt{p_1} + a_2\sqrt{p_2} + \dots + a_h\sqrt{p_h})^2 = a_1^2 p_1 + \dots + a_h^2 p_h + 2a_1 a_2 \sqrt{p_1 p_2} + 2a_1 a_3 \sqrt{p_1 p_3} + \dots =$$

$$= \sum_{i=1}^h a_i^2 p_i + \sum_{1 \leq i < j \leq h} 2a_i a_j \sqrt{p_i p_j}$$

$$p_i \in \mathbb{Z} \Rightarrow \sum_{1 \leq i < j \leq h} 2a_i a_j \sqrt{p_i p_j} \in \mathbb{Z} \subseteq \mathbb{Q}$$

Dimostriamo che cio' e' assurdo per $h = 2$:

$$\begin{aligned} \sum_{1 \leq i < j \leq 2} 2a_i a_j \sqrt{p_i p_j} &= 2a_1 a_2 \sqrt{p_1 p_2} \in \mathbb{Q} \Rightarrow \underbrace{\sqrt{p_1 p_2}}_{a_1, a_2 \in \mathbb{Q}} \in \mathbb{Q} \Rightarrow \\ &\Rightarrow \underbrace{k}_{p_i \text{ primo}} = p_1 \vee k = p_2 \Rightarrow p_1 p_2 = p_1^2 \vee p_1 p_2 = p_2^2 \Rightarrow p_2 = p_1 \end{aligned}$$

assurdo.

(1.2) Metodo 2.

Sia $n \in \mathbb{N}$, $n \geq 1$. Consideriamo il polinomio $f_n(x) = x^n - p \in \mathbb{Q}[x]$ con p primo. Per il Criterio di Eisenstein, $f_n(x)$ e' irriducibile in $\mathbb{Q}[x]$.

$$\begin{cases} f_n(x) \in \mathbb{Q}[x] \text{ irrid.} \\ f_n(x) \text{ monico} \\ f_n(\sqrt[n]{p}) = 0 \end{cases} \Rightarrow \underbrace{f_n(x) = P_{\min}(\sqrt[n]{p}, \mathbb{Q})}_{[2.30, \text{pg.24}]} \Rightarrow [\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n \quad (*)$$

$$f_n(x) \in \mathbb{Q}[x] \subseteq \overline{\mathbb{Q}}[x] \Rightarrow \underbrace{\sqrt[n]{p} \in \overline{\mathbb{Q}}}_{\overline{\mathbb{Q}} \text{ e' chiuso, [2.56, pg.42]}} \Rightarrow$$

$$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{p}) \subseteq \overline{\mathbb{Q}} \Rightarrow [\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$$

Per l'arbitrarieta' di n , deduciamo che $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ non puo' essere finita.

(2) $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ e' normale

Sia $f(x) \in \overline{\mathbb{Q}}[x]$ irriducibile, $\alpha \in \overline{\mathbb{Q}} : f(\alpha) = 0$, si ha

$$f(x) \text{ irrid. in } \overline{\mathbb{Q}}[x] \Rightarrow \underbrace{\deg f(x) = 1}_{[2.56, \text{pg.42}]} \Leftrightarrow f(x) = x - \alpha$$

quindi tutte le radici di $f(x)$ sono in $\overline{\mathbb{Q}}$.

Per l'arbitrarieta' di $f(x)$, e per definizione, $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ e' normale. □

Example 8.8. 1. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ non e' normale

2. $\mathbb{Z}_3(u) \preceq \mathbb{Z}_3(t)$, e' normale, dove $u = t^3$, t trascendente su $\mathbb{Z}_3$.

Proof:

(1) Dim 1.

Basta procedere come nell'esempio [5.4,pg.76], considerando che

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

(2) Dim 2.

$$\begin{aligned} \text{Sia } F = \mathbb{Z}_3(u), K = \mathbb{Z}_3(t), f(x) = x^3 - u \in F[x] \\ f(x) = x^3 - u = x^3 - t^3 \underbrace{=}_{[1.20, \text{pg.7}]} (x - t)^3 \in \mathbb{Z}_3(t)[x] \end{aligned}$$

$$F(t) = \mathbb{Z}_3(u)(t) = \mathbb{Z}_3(t, u) \underbrace{=}_{u \in \mathbb{Z}_3(t)} \mathbb{Z}_3(t) = K \Rightarrow K = F(t)$$

$$\Rightarrow K = \mathbb{Z}_3(t) = CS(f(x), F) \underbrace{\Rightarrow}_{[5.5, \text{pg.76}]} F \preceq K \text{ e' normale e finita}$$

□

Example 8.9. Sia $F = \mathbb{Z}_3(t, u)$, t, u trascendenti su $\mathbb{Z}_3$, $f(x) = (x^2 - t)(x^3 - u)$, $K = CS(f(x), F)$, $\alpha, \beta \in K$, $\alpha^2 = t, \beta^2 = u$. Si ha

$$x^2 - t = P_{\min}(\alpha, F), \text{ e' separabile}$$

$$x^3 - u = P_{\min}(\beta, F) \text{ e' non separabile}$$

Proof:

(1) Dim 1.

Sia $f(x) = x^2 - t$. Poiche' $f(\alpha) = 0$, $f(x)$ monico, basta dimostrare che $x^2 - t$ e' irriducibile in $F[x]$. E questo si vede usando il Criterio di Eisenstein cosi' come e' stato fatto nella dim della prop [3.28,pg.63].

Inoltre

$$\alpha \neq 0 \text{ infatti, } \alpha = 0 \Rightarrow f(\alpha) = 0 = f(0) = -t \Rightarrow t = 0 \text{ assurdo}$$

$$D[x^2 - t] = 2x \underbrace{=}_{2 \in \mathbb{Z}_3} -x \Rightarrow f'(\alpha) = -\alpha \neq 0 \underbrace{\Rightarrow}_{[1.17, \text{pg.6}]} \alpha \text{ non e' radice multipla} \underbrace{\Rightarrow}_{\deg f=2} f(x) \text{ ha radici distinte}$$

(2) Dim 2.

Come prima si vede che $g(x) = x^3 - u = P_{\min}(\beta, F)$, inoltre

$$D[x^3 - u] = 3x^2 \underbrace{=}_{z \in \mathbb{Z}_3} 0$$

quindi per la prop [1.17,pg.6], $x^3 - u$ ha solo radici multiple e in particolare

$$x^3 - u = (x - \beta)^3$$

□

Example 8.10. Studiare $\mathcal{I}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$.

Proof: Sia $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $\alpha = \sqrt[3]{2}$
 α e' radice di $x^3 - 2 \Rightarrow F \preceq K$ e' algebrica

$\text{ch} F = 0$

$$\underbrace{\Rightarrow}_{[3.23, \text{pg.} 60]} F \preceq K \text{ separabile}$$

$$F \subseteq K \text{ e' finita e separabile} \quad \underbrace{\Rightarrow}_{[6.10, \text{pg.} 84]} |\mathcal{G}(K, F)| \leq |\mathcal{I}(K, F)| = [K : F] = \deg P_{\min}(\alpha, F) = \deg x^3 - 2 = 3$$

$$\varphi \in \mathcal{G}(K, F) \quad \underbrace{\subseteq}_{[6.4, \text{pg.} 79]} \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.6, \text{pg.} 80]} \varphi(\alpha) \text{ e' radice di } x^3 - 2 \quad \underbrace{\Leftrightarrow}_{[1.19, \text{pg.} 7]} \varphi(\alpha) = \alpha \vee \varphi(\alpha) = \omega\alpha \vee \varphi(\alpha) = \omega^2\alpha \quad (1)$$

$$\begin{cases} \varphi(\alpha) \in K = \mathbb{Q}(\sqrt[3]{2}) \\ \varphi \in \mathcal{G}(K, F) \\ \omega\alpha, \omega^2\alpha \notin \mathbb{Q}(\sqrt[3]{2}) \end{cases} \quad \varphi(\alpha) \neq \omega\alpha, \varphi(\alpha) \neq \omega^2\alpha \quad \underbrace{\Rightarrow}_{(1)} \varphi(\alpha) = \alpha \Rightarrow \varphi = \text{id}$$

$$\Rightarrow \mathcal{G}(K, F) = \{\text{id}\} \Rightarrow |\mathcal{G}(K, F)| = 1 \neq 3 = |\mathcal{I}(K, F)| \Rightarrow \mathcal{G}(K, F) \neq \mathcal{I}(K, F) \quad \underbrace{\Rightarrow}_{[6.15, \text{pg.} 87]} F \preceq K \text{ non e' normale} \quad \square$$

Example 8.11. Sia F campo, $f(x) \in F[x]$ irriducibile, $\deg f(x) = 3$, $L = CS(f(x), F)$. Siano $\alpha, \beta, \gamma \in L$ le radici di $f(x)$ (non necessariamente distinte).

1. Determinare i possibili valori di $[L : F]$

2. Supponiamo $f(x)$ non separabile

(a) Determinare $\text{ch} F$, $[L : F]$, $\mathcal{I}(L, F)$

3. Supponiamo $f(x)$ separabile.

(a) $\beta \in F(\alpha) \Leftrightarrow \gamma \in F(\alpha)$

(b) $L = F(\alpha, \beta)$

(c) Supponiamo $\beta \notin F(\alpha)$. Determinare $[L : F(\alpha)]$, $\mathcal{I}(L, F(\alpha))$

(d) Supponiamo $\beta \in F(\alpha)$. Determinare $[L : F]$, $\mathcal{I}(L, F)$

Proof:

(1) Dim. 1.

Sia $f(x) = a\bar{f}(x)$, $\bar{f}(x) \in F[x]$ monico.

$f(x) \in F[x]$ irrid. $\Rightarrow \bar{f}(x) \in F[x]$ irrid.

$f(\alpha) = 0 \Rightarrow \bar{f}(\alpha) = 0$, e analogamente $\bar{f}(\beta) = \bar{f}(\gamma) = 0$

$\bar{f}(x)$ e' monico

$$\underbrace{\Rightarrow}_{[2.30, \text{pg.} 24]} \bar{f}(x) = P_{\min}(\alpha, F) = P_{\min}(\beta, F) = P_{\min}(\gamma, F) \quad (1)$$

$$\begin{cases} F \subseteq F(\alpha) \subseteq L \\ [F(\alpha) : F] \end{cases} \quad \underbrace{=}_{[2.40, \text{pg.} 29]} \deg P_{\min}(\alpha, F) = \deg \bar{f}(x) = \deg f(x) = 3 \quad \underbrace{\Rightarrow}_{[2.18, \text{pg.} 16]} 3 \mid [L : F]$$

$$[L : F] \quad \underbrace{\leq}_{[2.51, \text{pg.} 38]} (\deg f(x))! = 3! = 6$$

$$\Rightarrow [L : F] = 3 \vee [L : F] = 6$$

(2) Dim. 2.

Applichiamo la prop. [3.25,pg.61]:

$$f(x) \text{ non separabile, irriducibile} \xRightarrow{[3.25,pg.61]} \begin{cases} \text{ch}F = p, \quad p \text{ primo} \\ \exists g(x) \in F[x] : f(x) = g(x^p) \end{cases}$$

Abbiamo

$$\begin{aligned} 3 = \deg f(x) &= \deg g(x^p) = \lambda p, \quad \lambda = \deg g(x) \\ 3 = \lambda p &\xRightarrow{3, p \text{ sono primi}} \lambda = 1, \quad 3 = p \end{aligned}$$

Quindi $\text{ch}F = 3$. Inoltre,

$$\lambda = 1 \Rightarrow g(x) = ax - b, \quad a, b \in F[x], \quad a \neq 0$$

$$f(x) = g(x^3) = ax^3 - b$$

$$\text{Sia } \beta \text{ una radice di } ax^3 - b \text{ ovvero } \beta^3 = \frac{b}{a}$$

$$f(x) = 0 \Leftrightarrow x^3 - \frac{b}{a} = 0 \Leftrightarrow x^3 - \beta^3 = 0$$

$$x^3 - \beta^3 \xRightarrow{\text{ch}F=3, [1.20,pg.7]} (x - \beta)^3$$

Quindi tutte le radici di $f(x)$ sono $\alpha = \beta = \gamma$

$$\Rightarrow L = CS(f(x), F) = F(\alpha) \Rightarrow [L : F] = \deg P_{\min}(\alpha, F) \xRightarrow{(1)} \deg \bar{f}(x) = 3$$

Consideriamo adesso $\mathcal{I}(L, F)$:

$$\begin{cases} P_{\min}(\alpha, F) \text{ ha solo una radice} \\ L = F(\alpha) \end{cases} \xRightarrow{[6.8,pg.81]} |\mathcal{I}(L, F)| = 1$$

$$\text{id} \in \mathcal{I}(L, F)$$

$$\Rightarrow \mathcal{I}(L, F) = \{\text{id}\}$$

(3) Dim. 3.

Stiamo supponendo $f(x)$ separabile, quindi $\alpha \neq \beta, \beta \neq \gamma, \gamma \neq \alpha$.

(3.1) Dim $\beta \in F(\alpha) \Rightarrow \gamma \in F(\alpha)$

$$\begin{cases} \beta \in F(\alpha) \\ \bar{f}(\beta) = 0 \\ \bar{f}(x) \in F[x] \subseteq F(\alpha)[x] \end{cases} \xRightarrow{\text{Ruffini}} \bar{f}(x) = (x - \beta)f'(x), \quad f'(x) \in F(\alpha)[x]$$

$$\deg f(x) = 3 \Rightarrow \deg f'(x) = 2$$

$$\bar{f}(\alpha) = 0 \Leftrightarrow (\alpha - \beta)f'(\alpha) = 0 \xRightarrow{\alpha \neq \beta} f'(\alpha) = 0$$

$$\begin{cases} \alpha \in F(\alpha) \\ f'(\alpha) = 0 \\ f'(x) \in F(\alpha)[x] \\ \deg f'(x) = 2 \end{cases} \xRightarrow{\text{Ruffini}} f'(x) = (x - \alpha)(x - c), \quad c \in F(\alpha) \quad (*)$$

$$\bar{f}(\gamma) = 0 \Leftrightarrow (\gamma - \beta)f'(\gamma) = 0 \xRightarrow{\gamma \neq \beta} f'(\gamma) = 0 \Leftrightarrow (\gamma - \alpha)(\gamma - c) = 0 \xRightarrow{\gamma \neq \alpha} \gamma = c \in F(\alpha)$$

(3.2) Dim $\gamma \in F(\alpha) \Rightarrow \beta \in F(\alpha)$

Basta scambiare γ con β nella dimostrazione precedente.

⟨3.3⟩ Dim. $L = F(\alpha, \beta)$

Se $\beta \in F(\alpha)$ oppure $\gamma \in F(\alpha)$, per quanto abbiamo visto abbiamo

$$\beta, \gamma \in F(\alpha) \Rightarrow L = F(\alpha, \beta, \gamma) = F(\alpha) = F(\alpha, \beta)$$

Supponiamo allora che $\beta \notin F(\alpha) \wedge \gamma \notin F(\alpha)$. Si ha,

$$F \subseteq F(\alpha) \subseteq F(\alpha, \beta) \subseteq F(\alpha, \beta, \gamma) = L$$

$$\Rightarrow \underbrace{[F(\alpha, \beta) : F]}_{[2.18, \text{pg.16}]} / [L : F] \quad (*)$$

$$[L : F] = 3 \vee [L : F] = 6$$

$$\Rightarrow [F(\alpha, \beta) : F] = 1, 2, 3, 6 \quad [\text{sono i possibili valori}] \quad (*')$$

$$[F(\alpha) : F] = \deg P_{\min}(\alpha, F) \underbrace{=}_{(1)} \deg \bar{f}(x) = 3$$

$$\beta \notin F(\alpha) \Rightarrow F(\alpha) \subsetneq F(\alpha, \beta) \Rightarrow [F(\alpha, \beta) : F] > [F(\alpha) : F] = 3 \quad (*'')$$

$$(*), (*'), (*'') \Rightarrow [F(\alpha, \beta) : F] = 6 = [L : F]$$

$$\begin{cases} F(\alpha, \beta) \subseteq L \\ [F(\alpha, \beta) : F] = [L : F] \end{cases} \Rightarrow L = F(\alpha, \beta)$$

Inoltre, sempre per la prop [2.18,pg.16] deduciamo che

$$[F(\alpha, \beta) : F(\alpha)] = 2 \quad (2)$$

(ci servira' in seguito).

⟨3.4⟩ Supponiamo $\beta \notin F(\alpha)$. Determiniamo $[L : F(\alpha)], \mathcal{I}(L, F(\alpha))$

Per quanto visto prima

$$L = F(\alpha, \beta)$$

$$\beta \notin F(\alpha) \underbrace{\Rightarrow}_{(2)} [F(\alpha, \beta) : F(\alpha)] = 2$$

$$[L : F(\alpha)] = 2$$

$$[F(\alpha)(\beta) : F(\alpha)] = 2 \Rightarrow \deg P_{\min}(\beta, F(\alpha)) = 2 \Rightarrow h(x) = P_{\min}(\beta, F(\alpha)) = (x - \beta)(x - \beta_2)$$

Per costruire $\mathcal{I}(L, F(\alpha))$ basta usare la prop [6.8,pg.81]: gli unici due elementi $\varphi_1, \varphi_2 \in \mathcal{I}(L, F(\alpha))$ sono rispettivamente determinati dalle seguenti assegnazioni:

$$\beta \xrightarrow{\mathcal{L}_1} \beta$$

$$\beta \xrightarrow{\mathcal{L}_2} \beta_2$$

⟨3.5⟩ Supponiamo $\beta \in F(\alpha)$. Determiniamo $[L : F], \mathcal{I}(L, F)$

Abbiamo

$$L = F(\alpha, \beta) \underbrace{=}_{\beta \in F(\alpha)} F(\alpha)$$

$$[L : F] = [F(\alpha) : F] = \deg P_{\min}(\alpha, F) \underbrace{=}_{(1)} \deg \bar{f} = 3$$

Ricordando che le radici di $\bar{f}$ sono α, β, γ , per costruire $\mathcal{I}(F(\alpha), F)$ usiamo sempre la prop [6.8,pg.81]: gli unici due elementi $\bar{f}_1, \bar{f}_2, \bar{f}_3 \in \mathcal{I}(L, F)$ sono rispettivamente determinati

dalle seguenti assegnazioni:

$$\alpha \xrightarrow{\bar{f}_1} \alpha$$

$$\alpha \xrightarrow{\bar{f}_2} \beta$$

$$\alpha \xrightarrow{\bar{f}_2} \gamma$$

□

Example 8.12. Sia F campo e x_1, x_2 due indeterminate.

1. Scrivere $x_1^3 + x_2^3$ come combinazione dei polinomi simmetrici elementari σ_1, σ_2
2. Siano α, β le radici $f(x) \in F[x]$, polinomio irriducibile, $\deg f(x) = 2$. Verificare che

$$\alpha^3 + \beta^3 \in F$$

Proof:

$$\sigma_1(x_1, x_2) = x_1 + x_2$$

$$\sigma_2(x_1, x_2) = x_1 x_2$$

$$\sigma_1 \sigma_2 = x_1^2 x_2 + x_1 x_2^2$$

$$\sigma_1^3 - 3\sigma_1 \sigma_2 = x_1^3 + 3x_1^2 x_2 + 3x_1 x_2^2 + x_2^3 - 3x_1^2 x_2 - 3x_1 x_2^2 = x_1^3 + x_2^3$$

Infine,

$$\begin{cases} x_1^3 + x_2^3 \text{ e' simmetrico } \in F[x_1, x_2] \\ \alpha, \beta \text{ sono tutte le radici di } f(x) \\ f(x) \in F[x] \end{cases} \underbrace{\Rightarrow}_{[5.1, \text{pg. 74}]} \alpha^3 + \beta^3 \in F$$

□

Example 8.13. Sia $f(x) = x^4 + 1 \in \mathbb{Z}_5[x]$

1. Fattorizzare $f(x)$ in $\mathbb{Z}_5[x]$
2. Determinare $L = CS(x^2 + 2, \mathbb{Z}_5)$
3. Verificare che $L = CS(f(x), \mathbb{Z}_5)$
4. Trovare una legge esplicita per il seguente isomorfismo

$$L \simeq \frac{\mathbb{Z}_5[x]}{(x^2 + x - 3)}$$

Proof:

(1) Dim. 1.

$$x^4 + 1 = x^4 - 4 = (x^2 - 2)(x^2 + 2)$$

(2) Dim. 2.

Sia $\bar{x}$ una radice di $x^2 + 2$, allora $-\bar{x}$ e' ancora radice, quindi

$$L = CS(x^2 + 2, \mathbb{Z}_5) = \mathbb{Z}_5(\bar{x})$$

(3) Dim. 3.

Osserviamo che

$$\bar{x} \text{ radice di } x^2 + 2 \Rightarrow \bar{x}^2 + 2 = 0 \Rightarrow \bar{x}^2 = -2$$

$$(2\bar{x})^2 = 4\bar{x}^2 = -8 = -3 = 2 \Rightarrow 2\bar{x} \text{ e' radice di } x^2 - 2$$

$$\text{Analogamente } -2\bar{x} \text{ e' radice di } x^2 - 2$$

Quindi tutte le radici di $f(x) = (x^2 - 2)(x^2 + 2)$ sono
 $\pm 2\bar{x}, \pm \bar{x}$

percio'

$$CS(f(x), \mathbb{Z}_5) = \mathbb{Z}_5(\bar{x}) = L$$

(4) Dim. 4.

$g(x) = x^2 + x - 3$ non ha radici in $\mathbb{Z}_5$ (basta verificare per tutti i possibili valori di $x \in \mathbb{Z}_5$), quindi, avendo grado 2, e' irriducibile in $\mathbb{Z}_5[x]$.

Sia $\underline{x} \in CS(g(x), \mathbb{Z}_5)$ una radice di $g(x)$.

$$\begin{cases} g(x) \text{ irrid. in } \mathbb{Z}_5[x] \\ g(x) \text{ monico} \\ g(\underline{x}) = 0 \end{cases} \Rightarrow g(x) = P_{\min}(\underline{x}, \mathbb{Z}_5) \xrightarrow{[2.37, \text{pg.27}]} \mathbb{Z}_5(\underline{x}) \xrightarrow{\deg g(x)=2} \{a + b\underline{x} \mid a, b \in \mathbb{Z}_5\} \simeq \frac{\mathbb{Z}_5[x]}{(g(x))}$$

Cerchiamo quindi un isomorfismo φ da $L = \mathbb{Z}_5(\bar{x})$ a $\mathbb{Z}_5(\underline{x})$. Poiche' φ e' un isomorfismo tra campi, deve essere

$$\varphi(1) = 1 \Rightarrow \varphi|_{\mathbb{Z}_5} = \text{id}$$

Conoscendo $\varphi(\bar{x})$ determiniamo tutta l'immagine di φ , infatti,

$$\alpha \in \mathbb{Z}_5(\bar{x}) \Rightarrow \alpha = a + b\bar{x}, \quad a, b \in \mathbb{Z}_5$$

$$\varphi(\alpha) = \varphi(a) + \varphi(b)\varphi(\bar{x}) \xrightarrow{\varphi|_{\mathbb{Z}_5} = \text{id}} a + b\varphi(\bar{x})$$

Poiche' φ preserva il prodotto, si deve avere:

$$\varphi(\bar{x})^2 = \varphi(\bar{x}^2) = \varphi(-2) = -2$$

$$\varphi(\bar{x}) \in \mathbb{Z}_5(\underline{x}) \Rightarrow \varphi(\bar{x}) = a + b\underline{x}, \quad a, b \in \mathbb{Z}_5$$

$$(a + b\underline{x})^2 = -2 \Leftrightarrow a^2 + b^2\underline{x}^2 + 2ab\underline{x} = -2$$

$$\underline{x} \text{ radice di } x^2 + x - 3 \Rightarrow \underline{x}^2 + \underline{x} - 3 = 0 \Leftrightarrow \underline{x}^2 = 3 - \underline{x}$$

$$a^2 + b^2\underline{x}^2 + 2ab\underline{x} = -2 \Leftrightarrow a^2 + 3b^2 - b^2\underline{x} + 2ab\underline{x} = -2 \Leftrightarrow \begin{cases} a^2 + 3b^2 = -2 \\ 2ab - b^2 = 0 \end{cases} \Leftrightarrow \begin{cases} a^2 + 3b^2 = 3 \\ b^2 = 2ab \end{cases}$$

Una soluzione di tale sistema e'

$$(a, b) = (1, 2)$$

Tutte le possibili soluzioni sono

$$(a, b) = \pm(1, 2)$$

Per ogni soluzione determiniamo cosi' una $\varphi(\bar{x})$ diversa. Abbiamo cosi' trovato 2 isomorfismi espliciti da L a $\mathbb{Z}_5(\underline{x})$. □

Example 8.14. 1. $\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2}), \mathbb{Q}) \simeq S_3$

2. Determinare tutti i campi L t.c. $\mathbb{Q} \preceq L \preceq \mathbb{Q}(\omega, \sqrt[3]{2})$

Proof: Sia $K = \mathbb{Q}(\omega, \sqrt[3]{2})$, $F = \mathbb{Q}$, $G = \mathcal{G}(K, F)$, $H = \mathcal{G}(K, L)$, $J = \mathcal{G}(L, \mathbb{Q})$.

(1) Dim 1.

$$\begin{aligned}
& \left\{ \begin{array}{l} \mathbb{Q}(\omega, \sqrt[3]{2}) \stackrel{[8.3, \text{pg.173}]}{=} CS(x^3 - 2, \mathbb{Q}) \\ \text{Le radici di } x^3 - 2 \text{ sono } \sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \Rightarrow x^3 - 2 \text{ separabile} \end{array} \right. \quad (1) \\
(1) \quad & \stackrel{[6.26, \text{pg.99}]}{\Rightarrow} G \hookrightarrow S_3 \\
(1) \quad & \stackrel{[6.19, \text{pg.92}]}{\Rightarrow} F \preceq K \text{ e' di Galois} \\
& \stackrel{[6.19, \text{pg.92}]}{\Rightarrow} |G| = |\mathcal{G}(K, F)| = [K : F] \stackrel{[8.3, \text{pg.173}]}{=} 6 \\
& \left\{ \begin{array}{l} |S_3| = 3! = 6 = |G| \\ G \hookrightarrow S_3 \end{array} \right. \Rightarrow G \simeq S_3
\end{aligned}$$

(2) Dim 2.

$$\left\{ \begin{array}{l} \mathbb{Q} \preceq L \preceq K \\ F \preceq K \text{ di Galois} \end{array} \right. \stackrel{[6.23, \text{pg.96}]}{\Rightarrow} L \preceq K \text{ e' di Galois} \quad (2)$$

Per sfruttare la corrispondenza di Galois dobbiamo trovare $G = \mathcal{G}(K, F)$. Per semplificare il compito, possiamo prima trovare dei sottogruppi di G e poi farne un opportuno prodotto per riottenere G .

(2.1) Determiniamo $H_1 = \mathcal{G}(K, \mathbb{Q}(\sqrt[3]{2}))$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq K \stackrel{(2)}{\Rightarrow} \mathbb{Q}(\sqrt[3]{2}) \subseteq K \text{ e' di Galois} \stackrel{[6.24, \text{pg.96}]}{\Rightarrow} \mathcal{G}(K, \mathbb{Q}(\sqrt[3]{2})) = \mathcal{I}(K, \mathbb{Q}(\sqrt[3]{2})) = \mathcal{I}(\mathbb{Q}(\sqrt[3]{2})(\omega), \mathbb{Q}(\sqrt[3]{2}))$$

Per la prop. [6.8, pg.81], gli elementi di $\mathcal{I}(K, \mathbb{Q}(\sqrt[3]{2}))$ sono determinati dalle seguenti assegnazioni:

$$\begin{aligned}
\omega & \xrightarrow{\varphi_1} \omega \\
\omega & \xrightarrow{\varphi_2} \omega^2
\end{aligned}$$

dove ω, ω^2 sono le radici di $P_{\min}(\omega, \mathbb{Q}(\sqrt[3]{2})) = x^2 + x + 1$.

Quindi $H_1 = \{\varphi_1 = \text{id}, \varphi_2\} = \langle \varphi_2 \rangle$

(2.2) Determiniamo $N = \mathcal{G}(K, \mathbb{Q}(\omega))$

Analogamente a prima, $\mathcal{G}(K, \mathbb{Q}(\omega)) = \mathcal{I}(K, \mathbb{Q}(\omega)) = \mathcal{I}(\mathbb{Q}(\omega)(\sqrt[3]{2}), \mathbb{Q}(\omega))$. Gli elementi di $\mathcal{I}(K, \mathbb{Q}(\omega))$ sono determinati dalle seguenti assegnazioni:

$$\begin{aligned}
\sqrt[3]{2} & \xrightarrow{\psi_1} \sqrt[3]{2} \\
\sqrt[3]{2} & \xrightarrow{\psi_2} \omega \sqrt[3]{2} \\
\sqrt[3]{2} & \xrightarrow{\psi_3} \omega^2 \sqrt[3]{2}
\end{aligned}$$

dove $\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}$ sono le radici di $P_{\min}(\sqrt[3]{2}, \mathbb{Q}(\omega)) = x^3 - 2$.

Quindi $N = \{\psi_1 = \text{id}, \psi_2, \psi_3\} = \langle \psi_2 \rangle$

(2.3) N e' normale in G

$$\mathbb{Q}(\omega) = CS(x^2 + x + 1, \mathbb{Q})$$

Le radici di $x^2 + x + 1$ sono $\omega, \omega^2 \Rightarrow x^2 + x + 1$ e' separabile

$$\underbrace{\Rightarrow}_{[6.19, \text{pg.92}]}\quad \mathbb{Q} \subseteq \mathbb{Q}(\omega) \text{ e' di Galois}$$

$$\left\{ \begin{array}{l} \mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq K \\ \mathbb{Q} \subseteq K \text{ di Galois} \\ \mathbb{Q} \subseteq \mathbb{Q}(\omega) \text{ di Galois} \end{array} \right. \quad \underbrace{\Rightarrow}_{[6.30, \text{pg.101}]}\quad \mathcal{G}(K, \mathbb{Q}(\omega)) = N \text{ e' normale in } G$$

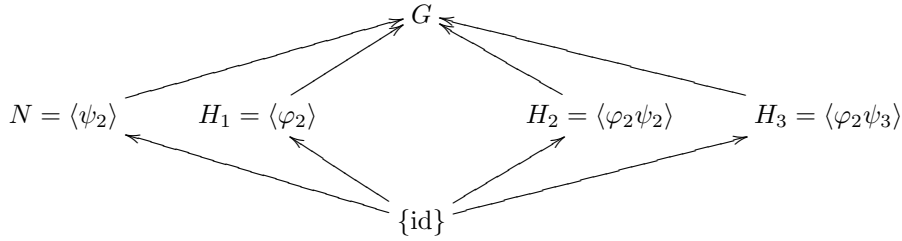
Quindi

$$\left\{ \begin{array}{l} H_1 \cap N = \{\text{id}\} \\ |H_1||N| = 6 = |G| \\ N \text{ e' normale} \end{array} \right. \quad \underbrace{\Rightarrow}_{[\text{AII}, 1.120, \text{pg.49}]}\quad G = H_1 N$$

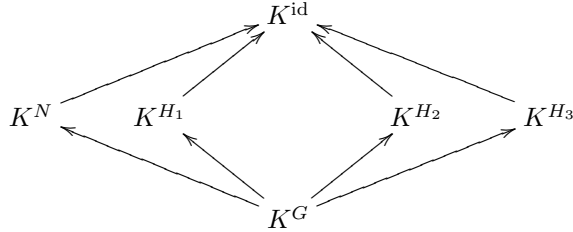
Abbiamo cosi' determinato G :

$$G = \{\text{id}, \psi_2, \psi_3, \varphi_2, \varphi_2\psi_2, \varphi_2\psi_3\}$$

Tutti i sottogruppi di G sono:



Determiniamo i corrispondenti campi intermedi usando la corrispondenza di Galois (vedi [6.25, pg.96], nota anche che le inclusioni vengono invertite):



Nello specifico:

$$K^{\text{id}} = K$$

$$K^G = K^{\mathcal{G}(K, F)} \quad \underbrace{=}_{F \preceq K \text{ e' di Galois, [6.19, pg.92]}} \quad = F$$

$$\mathbb{Q}(\sqrt[3]{2}) \subseteq K \text{ di Galois} \quad \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]}\quad K^{\mathcal{G}(K, \mathbb{Q}(\sqrt[3]{2}))} = \mathbb{Q}(\sqrt[3]{2}) \Leftrightarrow K^{H_1} = \mathbb{Q}(\sqrt[3]{2})$$

$$\mathbb{Q}(\omega) \subseteq K \text{ di Galois} \quad \underbrace{\Rightarrow}_{[6.19, \text{pg.92}]}\quad K^{\mathcal{G}(K, \mathbb{Q}(\omega))} = \mathbb{Q}(\omega) \Leftrightarrow K^N = \mathbb{Q}(\omega)$$

Per determinare i rimanenti K^{H_2}, K^{H_3} facciamo ricorso al campo coniugato:

$$\begin{cases} \psi_2 \in N \leq G = \mathcal{G}(K, F) = \mathcal{I}(K, F) \\ F \subseteq F(\sqrt[3]{2}) \subseteq K \end{cases} \xRightarrow{\substack{[6.34, \text{pg. } 106]}} \psi_2(F(\sqrt[3]{2})) = F(\psi_2(\sqrt[3]{2})) = \mathbb{Q}(\omega \sqrt[3]{2}) \quad (*)$$

$$\psi_2 H_1 \psi_2^{-1} = \psi_2 \mathcal{G}(K, \mathbb{Q}(\sqrt[3]{2})) \psi_2^{-1} \xRightarrow{\substack{[6.33, \text{pg. } 105]}} \mathcal{G}(K, \psi_2(\mathbb{Q}(\sqrt[3]{2}))) \xRightarrow{(*)} \mathcal{G}(K, \mathbb{Q}(\omega \sqrt[3]{2}))$$

$$\psi_2 H_1 \psi_2^{-1} = \{\text{id}, \psi_2 \varphi_2 \psi_2^{-1} = \psi_2 \varphi_2 \psi_3\}$$

$$\psi_2 \varphi_2 \psi_3 \text{ agisce così: } \begin{cases} \sqrt[3]{2} \xrightarrow{\psi_3} \omega^2 \sqrt[3]{2} \xrightarrow{\varphi_2} \omega^4 \sqrt[3]{2} = \omega \sqrt[3]{2} \xrightarrow{\psi_2} \omega^2 \sqrt[3]{2} \\ \omega \xrightarrow{\psi_3} \omega^2 \xrightarrow{\varphi_2} \omega^2 \xrightarrow{\psi_2} \omega^2 \end{cases}$$

$$\varphi_2 \psi_2 \text{ agisce così: } \begin{cases} \sqrt[3]{2} \xrightarrow{\psi_2} \omega \sqrt[3]{2} \xrightarrow{\varphi_2} \omega^2 \sqrt[3]{2} \\ \omega \xrightarrow{\psi_2} \omega \xrightarrow{\varphi_2} \omega^2 \end{cases}$$

$$\text{Quindi } \psi_2 \varphi_2 \psi_3 = \varphi_2 \psi_2 \Rightarrow \psi_2 H_1 \psi_2^{-1} = \{\text{id}, \psi_2 \varphi_2 \psi_3 = \varphi_2 \psi_2\} = \langle \varphi_2 \psi_2 \rangle = H_2$$

$$K^{H_2} = K^{\psi_2 H_1 \psi_2^{-1}} = K^{\mathcal{G}(K, \mathbb{Q}(\omega \sqrt[3]{2}))} \xRightarrow{=} \mathbb{Q}(\omega \sqrt[3]{2})$$

$\mathbb{Q}(\omega \sqrt[3]{2}) \subseteq K$ di Galois per la (2), [6.19, pg. 92]

$$K^{H_2} = \mathbb{Q}(\omega \sqrt[3]{2})$$

Analogamente:

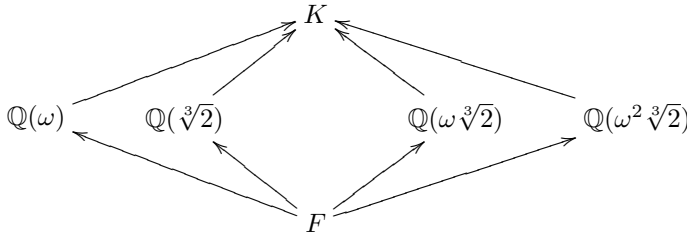
$$\psi_3(F(\sqrt[3]{2})) = \mathbb{Q}(\omega^2 \sqrt[3]{2})$$

$$\psi_3 H_1 \psi_3^{-1} = \mathcal{G}(K, \mathbb{Q}(\omega^2 \sqrt[3]{2}))$$

$$\psi_3 H_1 \psi_3^{-1} = \{\text{id}, \psi_3 \varphi_2 \psi_3^{-1} = \psi_3 \varphi_2 \psi_2 = \varphi_2 \psi_3\} = \langle \varphi_2 \psi_3 \rangle = H_3$$

$$K^{H_3} = \mathbb{Q}(\omega^2 \sqrt[3]{2})$$

Possiamo così riaggiornare il POSET dei campi di $F \preceq K$:



□

Example 8.15. 1. Studiare $\mathbb{C}(u) \preceq \mathbb{C}(t)$ con $u = t^n$, t indeterminata.

2. Verificare che

$$\mathcal{G}(\mathbb{C}(t), \mathbb{C}(u)) \xrightarrow[\text{isom. di gruppi}]{\simeq} U_n$$

dove $(U_n, \cdot)$ è il gruppo delle radici n -esime delle unità.

Proof: Sia $f(x) = x^n - u$. $f(x)$ e' irriducibile in $\mathbb{C}(u)[x]$ (nota³¹)

$$\begin{cases} f(x) \text{ irrid. in } \mathbb{C}(u)[x] \\ f(x) \text{ monico} \\ f(t) = 0 \end{cases} \Rightarrow f(x) = P_{\min}(t, \mathbb{C}(u))$$

Per la prop [1.19,pg.7], le radici di $f(x)$ sono

$$t, \omega t, \omega^2 t, \dots, \omega^{n-1} t$$

$$t \text{ indeterminata} \Rightarrow t \neq 0$$

quindi $f(x)$ e' anche separabile.

$$CS(f(x), \mathbb{C}(u)) = \mathbb{C}(u)(t, \omega t, \omega^2 t, \dots, \omega^{n-1} t) \underset{\omega^i \in \mathbb{C}}{=} \mathbb{C}(u, t) \underset{u=t^n \in \mathbb{C}(t)}{=} \mathbb{C}(t)$$

$$\begin{cases} \mathbb{C}(t) = CS(f(x), \mathbb{C}(u)) \\ f(x) \text{ separabile} \end{cases} \underset{[6.19,pg.92]}{\Rightarrow} \mathbb{C}(u) \preceq \mathbb{C}(t) \text{ di Galois} \quad (1)$$

$$(1) \underset{[6.19,pg.92]}{\Rightarrow} |\mathcal{G}(\mathbb{C}(t), \mathbb{C}(u))| = [\mathbb{C}(t) : \mathbb{C}(u)] = [\mathbb{C}(u)(t) : \mathbb{C}(u)] = \deg P_{\min}(t, \mathbb{C}(u)) = \deg f(x) = n$$

$$(1) \underset{[6.24,pg.96]}{\Rightarrow} \mathcal{G}(\mathbb{C}(t), \mathbb{C}(u)) = \mathcal{I}(\mathbb{C}(t), \mathbb{C}(u))$$

Per la prop. [6.8,pg.81], gli elementi di $\mathcal{I}(\mathbb{C}(t), \mathbb{C}(u))$ sono determinati dalle seguenti assegnazioni:

$$t \xrightarrow{\varphi_i} \omega^i t \quad \forall i = 0, \dots, n-1$$

Abbiamo anche che:

$$\mathcal{G}(\mathbb{C}(t), \mathbb{C}(u)) = \langle \varphi_1 \rangle, \text{ infatti,}$$

$$t \xrightarrow{\varphi_1} \omega t \xrightarrow{\varphi_1} \omega^2 t \xrightarrow{\varphi_1} \dots \xrightarrow{\varphi_1} \omega^{n-1} t \xrightarrow{\varphi_1} \omega^n t = t$$

$$\varphi_1^{n-1} \neq \text{id}, \varphi_1^n = \text{id} \Rightarrow o(\varphi_1) = n = |\mathcal{G}(\mathbb{C}(t), \mathbb{C}(u))|$$

$$\mathcal{G}(\mathbb{C}(t), \mathbb{C}(u)) \text{ ciclico} \Rightarrow \mathcal{G}(\mathbb{C}(t), \mathbb{C}(u)) \simeq \mathbb{Z}_n \underset{U_n \text{ e' ciclico}}{\simeq} U_n$$

□

Example 8.16. Studiare $\mathcal{G}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ sapendo che

$$\mathbb{Q}(i, \sqrt[4]{2}) = CS(x^4 - 2, \mathbb{Q})$$

A quale gruppo e' isomorfo?

Proof: TODO

□

³¹basta usare il criterio di Eisenstein cosi' come e' stato fatto nella dim della prop [3.28,pg.63]

9 *

Index

*, 188

Campi chiusi e chiusura, 42

Campi di spezzamento, 34

Campi finiti, 51

campo chiuso, 42

campo coniugato, 106

campo di spezzamento, 38

Caratteristica, 8

caratteristica, 9

catena risolvibile, 140

chiusura, 43

Ciclotomia, 133

corrispondenza di Galois, 98

Discriminante, 167

discriminante, 149

discriminante di f , 169

elemento

algebrico, 21

trascendente, 21

Esercizi, 172

estensione

di Galois, 96

finita, 16

finitamente generata, 20

normale, 76

semplice, 20

separabile, 59

estensione ciclica, 154

Estensione di Campi, 8

Estensioni, 15

Estensioni ciclotomiche, 112

Estensioni normali, 75

Estensioni risolubili, 147

Estensioni risolubili per radicali, 159

Estensioni separabili, 59

formule di Viete', 73

Gruppi risolubili, 140

Gruppo di Galois, 79

gruppo di Galois, 79

gruppo transitivo, 101

leading term, 71

norma, 148

ordinamento lessicografico, 70

Polinomi simmetrici, 70

polinomio derivato, 4

polinomio minimo, 23

Preliminari, 1

Proprieta' di $x^{p^n} - x$, 55

radici ennesime unita', 113

Riga e compasso, 120

Risolubilita' di S_n , 146

sottocampo fondamentale, 13

Teorema fondamentale dell'algebra, 108

traccia, 147

Zorn lemma, 7