

Complementi di Algebra

AlpT (@freaknet.org)

<http://freaknet.org/alpt>

June 5, 2008

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 ©2007 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	3
2.1	Caratteristica	3
2.2	Estensioni	6
2.3	Campi di spezzamento	12
2.4	Campi chiusi e chiusura	14
3	Campi finiti	16
3.1	Estensioni separabili	17
4	Polinomi simmetrici	20
5	Estensioni normali	22
6	Gruppo di Galois	23
6.1	Teorema fondamentale dell'algebra	29
6.2	Estensioni ciclotomiche	30
6.3	Riga e compasso	31
6.3.1	Ciclotomia	32
7	Gruppi risolubili	33
7.1	Risolubilita' di S_n	33
7.2	Estensioni risolubili	34
7.3	Estensioni risolubili per radicali	36
8	*	37

1 Preliminari

Utilizzeremo la teoria degli anelli (vedi [AI,17,pg.71]), la teoria dei gruppi (vedi [AI,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 .

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

$$K' \preceq K \Leftrightarrow \left\{ \begin{array}{l} (K', +) \leq (K, +) \\ \underbrace{\qquad\qquad\qquad}_{\text{sotto gruppo}} \\ (K'^*, \cdot) \leq (K^*, \cdot) \\ \underbrace{\qquad\qquad\qquad}_{\text{sotto gruppo}} \end{array} \right. \Leftrightarrow \forall a \in K' \left\{ \begin{array}{l} 1. a - b \in K' \quad \forall b \in K' \\ 2. ab^{-1} \in K' \quad \forall b \in K' \setminus \{0\} \end{array} \right.$$

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:

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

Proposition 1.9. Sia D un dominio, allora

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

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 .

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

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

Nota².

Proposition 1.12. Sia K un campo, allora

$$Q(K) \simeq K$$

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

$$\begin{aligned} \tilde{\varphi} : K[x] &\longrightarrow K'[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n \varphi(a_i) x^i \end{aligned}$$

si chiama omomorfismo indotto da φ .
 $\tilde{\varphi}$ e' un omomorfismo. Se φ e' iniettivo o suriettivo, anche $\tilde{\varphi}$ lo e'.

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

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

definiamo la sua derivata:

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

Dove l'operazione $i a_i$ e':

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

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

Nota³

Proposition 1.15. Valgono le usuali proprieta' 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. $D[f(g(x))] = f'(g(x))g'(x)$

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

³In realta', l'operazione $i a_i$ coincide con l'operazione di moltiplicazione del campo K . Vedi [2.12,pg.5]

Proposition 1.16.

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

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 molteplicità 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.

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

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

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

Definition 1.21. Lemma di Zorn.

Sia A un POSET,

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

Il lemma di Zorn è 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 $\gamma(1) = 1_A$.

Definition 2.2. Sia dato un anello unitario A , e sia γ la funzione definita in [2.1,pg.3], 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.91]] (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

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

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,

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

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

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

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

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.4], 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

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

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.

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

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

Proposition 2.9. Sia K un campo, per quanto abbiamo visto in [2.7,pg.5], $\text{ch}K = 0 \vee \text{ch}K = p$. Inoltre, si ha

$$\text{ch}K = p \text{ primo} \Rightarrow \mathbb{Z}_p \hookrightarrow K$$

$$\text{ch}K = 0 \Rightarrow \mathbb{Z} \hookrightarrow K, \quad \mathbb{Q} \hookrightarrow K$$

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

$$\text{ch}K = 0 \Rightarrow SF(K) \simeq \mathbb{Q}$$

$$\text{ch}K = p \text{ primo} \Rightarrow SF(K) \simeq \mathbb{Z}_p$$

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

$$n * a \stackrel{\text{def}}{=} \underbrace{a + a + \cdots + a}_{n\text{-volte}} = \underbrace{\bar{n}a}_{\text{moltiplicazione in } K}$$

$$\text{dove } \bar{n} = \begin{cases} n & SF(K) = \mathbb{Q} \Leftrightarrow \text{ch}K = 0 \\ [n]_p & SF(K) = \mathbb{Z}_p \Leftrightarrow \text{ch}K = p \\ \text{classe resto mod } p & \end{cases}$$

In seguito, per abuso di notazione, scriveremo:

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

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

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:

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

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

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

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:

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

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

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

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} (infatti⁵)

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

$$\begin{aligned} F_1 &= F \\ F_i &= F(\alpha_1, \dots, \alpha_{i-1}) \end{aligned}$$

si ha

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

ovvero:

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

⁵infatti, 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.

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

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.

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

Non vale il viceversa.

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

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

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

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

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

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 $\mathbb{Q}$.

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.

Proposition 2.27.

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

Non vale il viceversa.

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

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

$$\deg P(\alpha, F) = \{\deg f(x) \mid f(x) \in P(\alpha, F)\}$$

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

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

(Nota⁶)

Infine, vale

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

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.9]:

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

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:

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

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,

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

⁶Un polinomio e' monico quando il coefficiente dell'indeterminata di grado massimo e' 1

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.8],

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

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.9], $f(x)$ 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

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

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

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

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

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

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

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

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

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

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 .

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 $F[\alpha]$.

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:

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

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.11], si puo' ricavare la base di $F(\alpha)_F$.

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

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

Corollary 2.43. Nelle ipotesi della prop [2.42, pg.11], si ha

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

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

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

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

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

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.

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

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

2.3 Campi di spezzamento

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

$f(x)$ irriducibile in $F[x]$, $n \geq 1 \Rightarrow \exists F', K$ 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 .

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:

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

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 campo di spezzamento di $f(x)$ 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 $\alpha_1, \dots, \alpha_n$.

Nota⁷

Nota⁸

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 $n = \deg f(x)$.

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

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

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:

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

⁷poiche' $n = \deg f(x)$, per la 1. e per Ruffini (vedi [AI,16.1,pg.63]), $\alpha_1, \dots, \alpha_n$ sono tutte le radici di $f(x)$, anche se alcune potrebbero non essere distinte.

⁸Si ha

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

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

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 ⁹.

Proposition 2.54. *Dato $f(x) \in F[x]$,*

$$\begin{cases} K = CS(f(x), F) \\ F \preceq L \preceq K \end{cases} \Rightarrow K = CS(f(x), L)$$

2.4 Campi chiusi e chiusura

Definition 2.55. Sia F un campo.

F 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 $\Leftrightarrow F = K$

Definition 2.57. Sia $F \preceq \overline{F}$ una estensione. Poniamo

$$\overline{F} \text{ si chiama chiusura algebrica di } F \stackrel{\text{def}}{\Leftrightarrow} \begin{cases} F \preceq \overline{F} \text{ estensione algebrica} \\ \overline{F} \text{ algebricamente chiuso} \end{cases}$$

Lemma 2.58. *Sia*

1. $F \preceq L \preceq K = L(\alpha)$, con $\alpha \in K$ algebrico su L
2. $p(x) = P_{\min}(\alpha, L)$, $n = \deg p(x)$

⁹Nella definizione [2.50,pg.13] 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

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

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.2]), ovvero

$$\begin{aligned}\Phi : L[x] &\longrightarrow \overline{F}[x] \\ \sum_{i=0}^r a_i x^i &\mapsto \sum_{i=0}^r \varphi(a_i) x^i\end{aligned}$$

5. Sia $\overline{\beta}$ una radice di $\Phi(p)$

6. Sia data la seguente legge:

$$\begin{aligned}f : K = L(\alpha) &\longrightarrow \overline{F} \\ b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} &\mapsto \varphi(b_0) + \varphi(b_1)\overline{\beta} + \varphi(b_2)\overline{\beta}^2 + \cdots + \varphi(b_{n-1})\overline{\beta}^{n-1}\end{aligned}$$

o equivalentemente:

$$\begin{aligned}h(x) &\in L[x] \\ f(h(\alpha)) &= \Phi(h)(\overline{\beta})\end{aligned}$$

Allora,

$$f \text{ e' un omomorfismo t.c. } f|_L = \varphi$$

Theorem 2.59. Sia F un campo, allora

1. $\exists \overline{F}$ chiusura algebrica di F
2. $F \preceq K$ estensione algebrica $\Rightarrow \exists \varphi : K \hookrightarrow \overline{F}, \varphi|_F = \text{id}$
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 $\overline{F}$.

Example 2.60.

1. $\mathbb{C} = \overline{\mathbb{R}}$, infatti

$$\begin{aligned}\mathbb{R} &\underbrace{\preceq}_{[2.17, \text{pg.6}]} \mathbb{C} \text{ e' finita} && \underbrace{\Rightarrow}_{[2.44, \text{pg.11}]} \mathbb{R} \preceq \mathbb{C} \text{ algebrica} \\ &\mathbb{C} \text{ e' chiuso vedi [6.38,pg.30]}\end{aligned}$$

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. $\forall f(x) \in F[x] : \deg f(x) \geq 1 \quad f(x) \text{ si spezza linearmente in } K$
allora

$$K = \overline{F}$$

Proposition 2.62. *Sia $F \preceq K$ una estensione, allora*

$$F \preceq K \text{ algebrica} \Rightarrow \overline{K} = \overline{F}$$

Proposition 2.63. *Sia $F \preceq K$ estensione, si ha*

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

Example 2.64.

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

Basta applicare la prop [2.63,pg.16] considerando l'estensione $\mathbb{Q} \preceq \mathbb{C}$, e il thm [6.38,pg.30].

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*

$$\begin{cases} |F| = p \\ \dim_F K = n \end{cases} \Rightarrow |K| = p^n$$

Proposition 3.3.

$$K \text{ campo finito} \Rightarrow \begin{cases} \text{ch} K = p \\ |K| = p^n, \quad p \text{ primo}, n \in \mathbb{N}^* \end{cases}$$

Proposition 3.4. *Sia K campo.*

$$|K| = p^n, \quad p \text{ primo} \Rightarrow K = CS(x^{p^n} - x, \mathbb{Z}_p) = \{\alpha \mid \alpha^{p^n} - \alpha = 0\}$$

Corollary 3.5. *Siano K, K' campi, allora*

$$|K| = |K'| < \infty \Rightarrow K \simeq K'$$

Proposition 3.6. *Sia $p, n \in \mathbb{N}^*$, p primo. Sia $f(x) \in \mathbb{Z}_p[x]$, $n = \deg f(x)$*

$$f(x) \text{ irriducibile in } \mathbb{Z}_p \Rightarrow \begin{cases} \frac{\mathbb{Z}_p[x]}{(f(x))} \simeq \mathbb{Z}_p(\alpha) \quad \text{e' un campo} \\ |\mathbb{Z}_p(\alpha)| = p^n \\ \dim_{\mathbb{Z}_p} \mathbb{Z}_p(\alpha) = n \end{cases}$$

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 .

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.16], se $f(x) \in \mathbb{Z}_p[x]$ e' irriducibile, con $\deg f(x) = n$, un tale K sara'

$$K = \mathbb{Z}_p(\alpha), \quad \text{con } f(\alpha) = 0$$

Proposition 3.8. Sia K campo,

$$|K| < \infty \Rightarrow (K^*, \cdot) \text{ e' un gruppo ciclico}$$

Proposition 3.9. Sia p primo

$$\forall n \in \mathbb{N}, n \geq 2 \quad \exists f(x) \in \mathbb{Z}_p[x] \text{ irriducibile, } \deg f(x) = n$$

3.1 Estensioni separabili

Definition 3.10. 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 3.11. Sia $F[x]$ campo, $f(x), g(x) \in F[x]$, si ha

$$\begin{cases} f(x) \text{ separabile} \\ g(x) \not\mid f(x) \end{cases} \Rightarrow g(x) \text{ separabile}$$

Proposition 3.12. Sia $F \preceq K$ una estensione, $f(x), g(x) \in F[x]$. Siano inoltre

$$d_1(x) = \text{MCD}(f(x), g(x)) \in F[x] \text{ il massimo comune divisore in } F[x], \text{ ovvero}$$

$$d_1(x) \not\mid f(x), \quad d_2(x) \not\mid g(x) \text{ in } F[x], \text{ ovvero}$$

$$\begin{cases} f(x) = \lambda(x)d_1(x), & \lambda(x), d_1(x) \in F[x] \\ g(x) = \mu(x)d_2(x), & \mu(x) \in F[x] \end{cases}$$

$$d_2(x) = \text{MCD}(f(x), g(x)) \in K[x]$$

allora

$$d_1(x) = d_2(x)$$

In pratica, il MCD non varia all'interno di una estensione.

Proposition 3.13. *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.2]).

Proposition 3.14. *Sia F campo,*

$$\begin{cases} \text{ch}F = 0 \\ g(x) \in F[x] \text{ e' irriducibile} \end{cases} \Rightarrow g(x) \text{ e' separabile}$$

Proposition 3.15. *Sia F campo.*

$$\begin{cases} \text{ch}F = 0 \\ F \preceq K \text{ estensione algebrica} \end{cases} \Rightarrow F \preceq K \text{ e' separabile}$$

Proposition 3.16. *Sia F campo, $g(x) \in F[x]$, $n = \deg g(x)$. Si ha*

$$\begin{cases} \text{ch}F = p \\ g(x) \text{ irriducibile in } F[x] \\ p \nmid n \end{cases} \Rightarrow g(x) \text{ e' separabile}$$

Theorem 3.17. *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

$$f(x) = a_0 + a_1x^p + a_2x^{2p} + \dots + a_nx^{np} = \sum_{i=0}^n a_ix^{ip}$$

Corollary 3.18. *Sia F campo, $\text{ch}F = p$, p primo. Si ha*

$$f(x) \in F[x] \text{ irriducibile} \Rightarrow \exists g(x) \in F[x] \text{ irriducibile e separabile} : \exists e \in \mathbb{N} : f(x) = g(x^{p^e})$$

Proposition 3.19. *Sia $F \preceq K$ una estensione*

$$\begin{cases} F \text{ campo finito} \\ F \preceq K \text{ algebrica} \end{cases} \Rightarrow F \preceq K \text{ e' separabile}$$

Proposition 3.20. *Sia $F \preceq K$ una estensione*

$$\begin{aligned} F \preceq K \text{ separabile} &\Rightarrow F \preceq K \text{ algebrica} \\ F \preceq K \text{ separabile} &\nLeftarrow F \preceq K \text{ algebrica} \end{aligned}$$

Theorem 3.21. Sia $F \preceq K$ una estensione,

$$F \preceq K \text{ finitamente generata, separabile} \Rightarrow F \preceq K \text{ e' semplice}$$

In particolare, si ha

$$\begin{cases} F \text{ infinito} \\ K = F(\alpha, \beta), \alpha, \beta \in K \Rightarrow K = F(\alpha + \lambda\beta) \quad \forall \lambda \in F : \lambda \neq \frac{\alpha - \alpha_i}{\beta_j - \beta} \quad \forall i = 1, \dots, n, \quad \forall j = 2, \dots, m \\ F \preceq K \text{ separabile} \end{cases}$$

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 $P_{\min}(\beta, F)$

Example 3.22. 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:

$$x^p - u, \quad x^p - w \in F[x]$$

$$t, v \text{ algebrici su } F \xRightarrow{\text{[2.43,pg.11]}} F \preceq F(t, v) \text{ algebrica} \xRightarrow{\text{[2.42,pg.11]}} F \preceq F(t, v) \text{ finita}$$

Analogamente a quanto fatto nella dimostrazione [3.20,pg.18] (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 $\exists \gamma \in K : K = F(\gamma)$.

$$F \subseteq F(t) \subseteq F(t, v)$$

$$(1) \Rightarrow [F(t) : F] = p$$

$$(1.1) \Rightarrow [F(t, v) : F(t)] \leq p$$

$$(1.2) \Rightarrow \deg P_{\min}(v, F(t)) \geq p \Leftrightarrow [F(t, v) : F(t)] \geq p$$

$$\Rightarrow [F(t, v) : F(t)] = p$$

$$\begin{cases} [F(t) : F] = p \\ [F(t, v) : F(t)] = p \end{cases} \Rightarrow [F(t, v) : F] = p^2 \Leftrightarrow [K : F] = p^2 \quad (1)$$

Si ha

$$\begin{aligned}
\gamma \in K = F(t, v) &\stackrel{\text{[2.21, pg. 7]}}{\Rightarrow} \gamma = \frac{f(t, v)}{g(t, v)} = \frac{a_{00} + a_{01}v + a_{02}v^2 + \dots + a_{10}t + a_{11}tv + a_{21}t^2v + \dots}{b_{00} + b_{01}v + b_{02}v^2 + \dots + b_{10}t + b_{11}tv + b_{21}t^2v + \dots} \\
\gamma^p &\stackrel{\text{[1.20, pg. 3]}}{=} \frac{a_{00}^p + a_{01}^p v^p + a_{02}^p v^{2p} + \dots + a_{10}^p t^p + a_{11}^p t^p v^p + a_{21}^p t^{2p} v^p + \dots}{b_{00}^p + b_{01}^p v^p + b_{02}^p v^{2p} + \dots + b_{10}^p t^p + b_{11}^p t^p v^p + b_{21}^p t^{2p} v^p + \dots} = \\
&= \frac{a_{00}^p + a_{01}^p w + a_{02}^p w^2 + \dots + a_{10}^p u + a_{11}^p uw + a_{21}^p u^2 w + \dots}{b_{00}^p + b_{01}^p w + b_{02}^p w^2 + \dots + b_{10}^p u + b_{11}^p uw + b_{21}^p u^2 w + \dots} = \frac{\bar{f}(u, w)}{\bar{g}(u, w)} \in \mathbb{Z}_p(u, w) = F \Rightarrow \\
&\Rightarrow \gamma \text{ e' radice di } x^p - \frac{\bar{f}(u, w)}{\bar{g}(u, w)} \in F[x] \Rightarrow \deg P_{\min}(\gamma, F) \leq p \Rightarrow [F(\gamma) : F] \leq p \Leftrightarrow [K : F] \leq p
\end{aligned}$$

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 [3.21, pg. 19], possiamo dedurre che $F \preceq K$ non e' separabile.

Theorem 3.23. 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 3.24.

$$\begin{cases} F \preceq L \text{ separabile} \\ F \preceq K \preceq L \end{cases} \Rightarrow \begin{cases} F \preceq K \\ K \preceq L \end{cases} \text{ separabili}$$

Proposition 3.25.

$$\begin{cases} F \preceq F(\alpha_1, \dots, \alpha_n) \\ \alpha_i \text{ separabile su } F \quad \forall i = 1, \dots, n \end{cases} \Rightarrow F \preceq F(\alpha_1, \dots, \alpha_n) \text{ e' separabile}$$

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

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 $f(\underline{x})$:

$$\text{LT}(f) \text{ e' il termine di } f(\underline{x}) \text{ t.c. } a \leq \text{LT}(f) \quad \forall a(\underline{x}) \text{ termine di } f(\underline{x})$$

ovvero

$$\text{LT}(f) = \max_{\leq} \{a(\underline{x}) \text{ termine di } f(\underline{x})\}$$

Poiche' $\leq$ e' un ordinamento totale (vedi [4.2,pg.21]), $\text{LT}(f)$ esiste ed e' unico.

Proposition 4.4. Sia $f, g \in F[x_1, \dots, x_n]$, si ha

$$\begin{aligned}\text{LT}(fg) &= \text{LT}(f)\text{LT}(g) \\ \text{LT}(f^m) &= \text{LT}(f)^m \quad \forall m \in \mathbb{N}\end{aligned}$$

Definition 4.5. Sia $f \in F[x_1, \dots, x_n]$, $\underline{x} = (x_1, \dots, x_n)$.

$$\begin{aligned}f \text{ e' simmetrico} &\stackrel{\text{def}}{\iff} f(\underline{x}) = f(\sigma(\underline{x})) \quad \forall \sigma \in S_n \\ \text{dove } \sigma(\underline{x}) &= (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})\end{aligned}$$

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:

$$\begin{aligned}\sigma_1(x_1, \dots, x_n) &= x_1 + x_2 + \dots + x_n \\ \sigma_2(x_1, \dots, x_n) &= \sum_{i < j} x_i x_j \\ \sigma_3(x_1, \dots, x_n) &= \sum_{i_1 < i_2 < i_3} x_{i_1} x_{i_2} x_{i_3} \\ &\dots \\ \sigma_h(x_1, \dots, x_n) &= \sum_{i_1 < i_2 < \dots < i_h} x_{i_1} x_{i_2} \dots x_{i_h} \\ &\dots \\ \sigma_n(x_1, \dots, x_n) &= x_1 x_2 \dots x_n\end{aligned}$$

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.

$$\text{LT}(\sigma_h) = x_1 x_2 \dots x_h$$

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.

Theorem 4.8. Sia $f \in F[x_1, \dots, x_n]$ un polinomio simmetrico, $\underline{x} = (x_1, \dots, x_n)$. Si ha

$$\exists! g \in F[x_1, \dots, x_n] : g(\sigma_1(\underline{x}), \sigma_2(\underline{x}), \dots, \sigma_n(\underline{x}))$$

Dove σ_i sono i polinomi simmetrici elementari.

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

$$p(\underline{x}) \text{ simmetrico} \Rightarrow p(\alpha_1, \dots, \alpha_d) \in F$$

$$\text{dove } \alpha_1, \dots, \alpha_d \in K \text{ sono tutte le radici di } f(x)$$

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*

$$\forall f(x) \in F[x] \quad F \preceq CS(f(x), F) \text{ e' normale}$$

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

$$F \preceq K \text{ normale, finita} \Rightarrow K = CS\left(\prod_{i=1}^n P_{\min}(\alpha_i, F), F\right)$$

Proposition 5.6. *Sia $F \preceq K$ una estensione,*

$$[K : F] = 2 \Rightarrow F \preceq K \text{ e' normale}$$

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.

$$\begin{aligned} \mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) &= \{\text{id}, f\} \\ \text{con } f(a + ib) &= a - ib \end{aligned}$$

Proposition 6.3. *Sia $F \preceq K$ algebrica. Si ha*

$$\begin{aligned} \varphi \in \mathcal{I}(K, F) &\Rightarrow \varphi : K_F \longrightarrow \overline{F}_F \text{ e' una applicazione lineare iniettiva} \\ \varphi \in \mathcal{G}(K, F) &\Rightarrow \varphi : K_F \longrightarrow K_F \text{ e' un isomorfismo vettoriale} \end{aligned}$$

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.

Proposition 6.5.

$$\begin{cases} F \preceq K \text{ algebrica} \\ F \preceq L \preceq K \end{cases} \Rightarrow \mathcal{I}(K, L) \subseteq \mathcal{I}(K, F)$$

Proposition 6.6. *Sia*

1. $F \preceq K$ algebrica, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$
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. 2])

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. $\tilde{\varphi}(\alpha)$ 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

$$\begin{aligned} \tilde{\varphi}(f(a)) &= f(\tilde{\varphi}(a)) \\ \tilde{\varphi}(\alpha) &\text{ e' radice di } p(x) \end{aligned}$$

Proposition 6.7. *Sia $F \preceq K$ algebrica, $\alpha \in K$, $p(x) = P_{\min}(\alpha, F)$, $\tilde{\varphi} \in \mathcal{I}(K, F)$, allora si ha*

$$\tilde{\varphi}(\alpha) \text{ e' radice di } p(x)$$

Preso $f(x) \in F[x]$, $a \in K$, si ha

$$\tilde{\varphi}(f(a)) = f(\tilde{\varphi}(a))$$

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

$$\begin{aligned} \begin{cases} K = F(\alpha) \\ \alpha \text{ algebrico su } F \end{cases} &\Rightarrow \begin{cases} |E| \leq n \\ |E| = |\{ \tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E \}| \text{ con biezione } \tilde{\varphi} \in E \mapsto \tilde{\varphi}(\alpha) \\ \{ \beta_1, \dots, \beta_n \} = \{ \tilde{\varphi}(\alpha) \mid \tilde{\varphi} \in E \} \end{cases} \\ \begin{cases} K = F(\alpha) \\ \alpha \text{ separabile e algebrico su } F \end{cases} &\Rightarrow |E| = n \end{aligned}$$

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.

Corollary 6.10.

$$\begin{aligned} F \preceq K \text{ finita} &\Rightarrow |\mathcal{G}(K, F)| \leq |\mathcal{I}(K, F)| \leq [K : F] \\ F \preceq K \text{ finita e separabile} &\Rightarrow |\mathcal{G}(K, F)| \leq |\mathcal{I}(K, F)| = [K : F] \end{aligned}$$

Definition 6.11. Sia $F \preceq K$ algebrica e $T \subseteq \mathcal{I}(K, F)$, definiamo

$$K^T = \{\alpha \in K \mid t(\alpha) = \alpha \ \forall t \in T\}$$

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

Proposition 6.13. Sia $F \preceq L \preceq K$, si ha

$$F \preceq K \text{ separabile, finita} \Rightarrow L = K^{\mathcal{I}(K, L)}$$

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'

$$f(L) = \mathcal{I}(K, L)$$

Proposition 6.15.

$$F \preceq K \text{ finita e normale} \Rightarrow \mathcal{G}(K, F) = \mathcal{I}(K, F)$$

Example 6.16.

$$\begin{aligned} \mathcal{G}(\mathbb{Q}(i), \mathbb{Q}) &= \mathcal{I}(\mathbb{Q}(i), \mathbb{Q}) = \{\text{id}, f\} \\ \text{con } f(a + ib) &= a - ib \end{aligned}$$

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 $H = G$.

Lemma 6.18.

$$\begin{cases} F \preceq K \text{ algebrica} \\ K = F(\alpha_1, \dots, \alpha_n) \\ \alpha_1, \dots, \alpha_n \in K, \quad \text{separabili su } F \end{cases} \Rightarrow \exists \gamma \in K \text{ separabile su } F \text{ t.c. } K = F(\gamma)$$

*Nota*¹⁰

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. $K = CS(f(x), F)$
3. $F \preceq L \preceq K \Rightarrow |\mathcal{G}(K, L)| = [K : L]$
4. $F = K^{\mathcal{G}(K, F)}$
5. $|\mathcal{G}(K, F)| = [K : F]$

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.26]

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.

¹⁰a differenza del thm [3.21,pg.19], stiamo affermando che γ e' separabile e non stiamo richiedendo che $F \preceq K$ sia separabile.

Proposition 6.22.

$$\begin{cases} F \preceq K \text{ e' di Galois} \\ F \preceq L \preceq K \end{cases} \Rightarrow L \preceq K \text{ e' di Galois, ma non e' detto che pure } F \preceq L \text{ lo sia}$$

Proposition 6.23. Sia $F \preceq K$ una estensione di Galois. Si ha

$$\mathcal{G}(K, F) = \mathcal{I}(K, F)$$

Theorem 6.24. Corrispondenza di Galois.

Sia $F \preceq K$ una estensione di Galois, allora

$$\begin{aligned} \left| \{L \mid F \preceq L \preceq K\} \right| &= \left| \{H \mid H \leq \mathcal{G}(K, F) \text{ sottogruppo}\} \right| \\ \text{In particolare, un funzione biettiva tra i due insiemi e'} \\ f(L) &= \mathcal{G}(K, L) \\ f^{-1}(H) &= K^H \end{aligned}$$

Proposition 6.25. 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 .

Corollary 6.26. Sia $f(x) \in F[x]$ separabile, $K = CS(f(x), F)$, $\deg f(x) = n$. Si ha

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

Definition 6.27. Sia H un gruppo di funzioni e A un insieme non vuoto.

$$H \text{ e' transitivo su } A \stackrel{\text{def}}{\Leftrightarrow} \forall \alpha_i, \alpha_j \in A \exists \sigma \in H : \sigma(\alpha_i) = \alpha_j$$

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 6.28. 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 [6.25, pg. 27], $G \simeq H \leq S_n$. 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 .

Theorem 6.29. 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

Corollary 6.30. 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

Proposition 6.31. 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 .

Proposition 6.32. Sia $F \preceq K$ di Galois, $F \preceq L \preceq K$, $\varphi \in G = \mathcal{G}(K, F)$. Si ha

$$\mathcal{G}(K, \varphi(L)) = \varphi \mathcal{G}(K, L) \varphi^{-1}$$

$$\text{dove } \varphi \mathcal{G}(K, L) \varphi^{-1} \stackrel{\text{def}}{=} \{ \varphi g \varphi^{-1} \mid g \in \mathcal{G}(K, L) \}$$

Proposition 6.33. 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

$$\varphi(L) = \varphi(F(\alpha_1, \dots, \alpha_n)) = F(\beta_1, \dots, \beta_n)$$

6.1 Teorema fondamentale dell'algebra

Proposition 6.34.

$$\mathbb{C} \text{ e' chiuso} \Leftrightarrow (f(x) \in \mathbb{R}[x], \deg f(x) \geq 1 \Rightarrow \exists \alpha \in \mathbb{C} : f(\alpha) = 0)$$

Proposition 6.35. Sia $f(x) \in \mathbb{R}[x]$, allora

$$\deg f(x) \text{ dispari} \Rightarrow \exists \alpha \in \mathbb{R} : f(\alpha) = 0$$

Proposition 6.36.

$$f(x) = a_0 + \dots + a_d x^d, \quad d \text{ dispari}$$

Supponiamo $a_d > 0$ (analogamente si vede per $a_d < 0$). Si ha

$$\lim_{x \rightarrow \infty} f(x) = \lim_{x \rightarrow \infty} a_d x^d \underbrace{=}_{a_d > 0} + \infty$$

Quindi, definitivamente $f(x)$ sara' positivo. Allora esiste $b \in \mathbb{R} : f(b) > 0$.

$$\lim_{x \rightarrow -\infty} f(x) = \lim_{x \rightarrow \infty} a_d x^d \underbrace{=}_{a_d > 0, d \text{ dispari}} -\infty$$

Quindi, definitivamente $f(x)$ sara' positivo. Allora esiste $a \in \mathbb{R} : f(a) < 0$.

$$\begin{cases} f(a)f(b) < 0 \\ f \text{ continua} \end{cases} \underbrace{\Rightarrow}_{\text{thm dell'esistenza dello zero}} \exists \alpha \in]\min\{a, b\}, \max\{a, b\}[: f(\alpha) = 0$$

Proposition 6.37. Sia $f(x) \in \mathbb{C}[x]$

$$\deg f(x) = 2 \Rightarrow f(x) \text{ si spezza linearmente in } \mathbb{C}[x]$$

Theorem 6.38.

$\mathbb{C}$ e' algebricamente chiuso

6.2 Estensioni ciclotomiche

Proposition 6.39. 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:

$$b, \omega_1 b, \omega_2 b, \dots, \omega_m b \in CS(f(x), F)$$

$$\text{dove } b^n = a, U_n = \{1, \omega_1, \dots, \omega_m\}$$

$(U_n, \cdot)$ e' il gruppo moltiplicativo delle radici n -esime dell'unita' nel campo F , ovvero

$$U_n = \{\xi \in CS(x^n - 1, F) \mid \xi^n - 1 = 0\}$$

Si distinguono allora i seguenti casi:

Theorem 6.40. Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unita'. Poniamo

$$f(x) = x^n - 1$$

$$f_m(x) = \prod_{u \in U_n : U_m = \langle u \rangle} x - u \quad \text{dove } m \mid n$$

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. $f(x) = \prod_{m \mid n} f_m(x)$
2. $f_n(x) \in \mathbb{Z}[x], f_n(x) = P_{\min}(\omega, \mathbb{Q})$
3. $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg f_n(x) = \varphi(n)$
4. $\mathbb{Q} \preceq \mathbb{Q}(\omega)$ e' di Galois

Proposition 6.41. 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

$$\mathcal{G}(\mathbb{Q}(\omega), \mathbb{Q}) \simeq U(\mathbb{Z}_n)$$

6.3 Riga e compasso

Definition 6.42. Sia $\mathbf{E} = \mathbb{R}^2$ il piano affine euclideo costruito sullo spazio vettoriale $\mathbb{R}^2$ (nota¹¹)

Una costruzione euclidea (con riga e compasso) e' una successione $A_0, \dots, A_n$ di punti, rette 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 $\Rightarrow \exists h, j, k < i : A_h, A_j, A_k \in \mathbf{E}, C(A_h, \|\overrightarrow{A_j A_k}\|) = A_i$
dove $\overrightarrow{A_j A_k}$ e' il vettore $A_k - A_j$
 $\|\overrightarrow{A_j A_k}\|$ e' la sua norma
 $C(A_h, \|\overrightarrow{A_j A_k}\|)$ 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 6.43.

$a \in \mathbb{R}$ 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

$$\mathbb{E} = \{a \in \mathbb{R} \mid a \text{ e' euclideo}\} \cup \{1\}$$

Proposition 6.44. *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 $P \in r$

Proposition 6.45.

$$a, b, c \in \mathbb{E}, c \neq 0 \Rightarrow b \pm a, ab, ac^{-1}, \sqrt{|a|} \in \mathbb{E}$$

Proposition 6.46.

$$\mathbb{Q} \leq \mathbb{E} \leq \mathbb{R}$$

¹¹e' in pratica l'usuale piano $\mathbb{R}^2$ dotato di prodotto scalare e quindi di norma, distanza, angoli. Vedi [GII, ??, pg. ??]

Proposition 6.47. 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 $A_0 = O = (0, 0)$, $A_1 = (1, 0)$.

Theorem 6.48.

$$a \in \mathbb{E} \Leftrightarrow \exists \text{ una catena di campi } \mathbb{Q} = K_0 \preceq K_1 \preceq \dots \preceq K_t \preceq \mathbb{R} \text{ tale che } \begin{cases} a \in K_t \\ t \geq 1 \Rightarrow [K_i : K_{i-1}] = 2 \quad \forall i = 1, \dots, t \end{cases}$$

Corollary 6.49.

$$a \in \mathbb{E} \Rightarrow a \text{ e' algebrico su } \mathbb{Q}, \quad \deg P_{\min}(a, \mathbb{Q}) = 2^m, \quad m \geq 0$$

Example 6.50.

1. E' impossibile rettificare la circonferenza
2. E' impossibile quadrare il cerchio
3. E' impossibile duplicare il cubo

6.3.1 Ciclotomia

Proposition 6.51. E' possibile costruire un poligono regolare di n lati inscritto nella circonferenza unitaria $\Leftrightarrow \omega$ e' euclideo, dove $U_n = \langle \omega \rangle$.

Proposition 6.52. Sia $U_n = \langle \omega \rangle$, allora

$$\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \text{ e' euclideo } \Leftrightarrow \cos \frac{2\pi}{n} \in \mathbb{E}$$

Theorem 6.53. 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.

Proposition 6.54. 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

$$\begin{aligned} \varphi(n) = 2^m &\Leftrightarrow \begin{cases} s_1 = s_2 = \dots = s_t = 1 \\ p_i = 2^{h_i} + 1 \quad \forall i = 1 \dots t \end{cases} \\ \varphi(n) = 2^m &\Rightarrow n = 2^{s_0} (2^{h_1} + 1) \dots (2^{h_t} + 1) \\ &\text{con } k_i, h_i \geq 0 \end{aligned}$$

Proposition 6.55. Sia dato il seguente algoritmo scritto in J¹²

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 risolvente*.

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

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 risolvente $\{e\} = H_0 \leq \dots \leq H_n = G$ t.c. $\left| \frac{H_i}{H_{i-1}} \right| = p_i$ primo $\forall i = 1, \dots, n$

Proposition 7.4. Sia G un gruppo, allora

$$\begin{cases} N \leq G \text{ normale} \\ N \text{ risolubile} \\ \frac{G}{N} \text{ risolubile} \end{cases} \Rightarrow G \text{ risolubile}$$

Theorem 7.5. di Feit-Thompson.

Sia G un gruppo, allora

$$|G| \text{ dispari} \Rightarrow G \text{ risolubile}$$

7.1 Risolubilita' di S_n

Proposition 7.6. S_n e' risolubile $\forall n = 1, \dots, 4$

Theorem 7.7. S_n non e' risolubile $\forall n \geq 5$

¹²Vedi Jsoftware <http://www.jsoftware.com/>

7.2 Estensioni risolubili

Definition 7.8. Sia $F \preceq K$ una estensione algebrica. Definiamo la *traccia* e *norma*.

$$\begin{aligned}\mathrm{Tr}_{K,F} : K &\longrightarrow \overline{F} \\ \mathrm{Tr}_{K,F}(\alpha) &= \sum_{\sigma \in \mathcal{I}(K,F)} \sigma(\alpha) \\ \mathcal{N}_{K,F} : K &\longrightarrow \overline{F} \\ \mathcal{N}_{K,F}(\alpha) &= \prod_{\sigma \in \mathcal{I}(K,F)} \sigma(\alpha)\end{aligned}$$

Proposition 7.9.

$$F \preceq K \text{ e' di Galois} \Rightarrow \mathrm{Tr}_{K,F}(\alpha), \mathcal{N}_{K,F}(\alpha) \in F$$

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.25] possiamo cosi' 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.34] e definita la seguente matrice

$$\begin{aligned}T &\in \overline{F}^{n \times n} \\ T_{ij} &= \mathrm{Tr}_{K,F}(a_i a_j)\end{aligned}$$

si ha

$$\begin{aligned}1. \quad &\Delta^2 = \det T \\ 2. \quad &\begin{cases} F \preceq K \text{ di Galois} \\ \mathrm{ch} F = 0 \end{cases} \Rightarrow \Delta \neq 0\end{aligned}$$

Proposition 7.12. Ponendoci nel contesto della def [7.10,pg.34], si ha

$$\begin{cases} F \preceq K \text{ di Galois} \\ \mathrm{ch} F = 0 \end{cases} \Rightarrow \sigma_1, \dots, \sigma_n \text{ sono l.i. su } F, \text{ ovvero } \begin{cases} \sigma_1, \dots, \sigma_n \in \mathrm{Hom}(K, F) = \text{spazio duale di } K_F \\ \mathcal{L}(\sigma_1, \dots, \sigma_n)_F = \mathrm{Hom}(K, F) \end{cases}$$

Proposition 7.13. Sia

$$1. \quad F \preceq K \text{ di Galois, } \mathrm{ch} F = 0, \text{ con } n = [K : F]$$

$$2. G = \mathcal{G}(K, F) = \langle \tau \rangle$$

allora, preso $\alpha \in K$, si ha

$$\mathcal{N}_{K,F}(\alpha) = 1 \Leftrightarrow \exists b \in K^* : \alpha = \frac{b}{\tau(b)}$$

Proposition 7.14. Sia $U_n = \langle \omega \rangle$ il gruppo delle radici n -esime dell'unità'.

$$\begin{cases} F \preceq K \text{ di Galois, } \text{ch}F = 0, [K : F] = n \\ G = \mathcal{G}(K, F) = \langle \tau \rangle \\ \omega \in F \end{cases} \Rightarrow \exists b \in K^* : K = F(b) = CS(x^n - b^n, F), b^n \in F$$

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',

$$\begin{cases} K = CS(x^n - a, F), a \in F^* \\ \omega \in F, \text{ch}F = 0 \end{cases} \Rightarrow \begin{cases} F \preceq K \text{ e' di Galois} \\ G = \mathcal{G}(K, F) \text{ e' ciclico} \\ [K : F] / n \end{cases}$$

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

$$K = F(b), b^n \in F^* \Leftrightarrow \begin{cases} F \preceq K \text{ e' ciclica e di Galois} \\ [K : F] / n \end{cases}$$

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 $\mathbb{Z}_n$.

Proposition 7.19. Sia

1. F campo, $\text{ch}F = 0$
2. $K = CS(x^n - a, F)$, $a \in F^*$

allora

$$\mathcal{G}(K, F) \text{ e' risolubile}$$

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

7.3 Estensioni risolubili per radicali

Definition 7.21. Sia $f(x) \in F[x]$, $L = CS(f(x), F)$,

$$f(x) \text{ e' risolubile per radicali} \stackrel{\text{def}}{\Leftrightarrow} \begin{cases} \exists K : L \preceq K = F(\alpha_1, \dots, \alpha_m) \\ a_1 \in F \\ \forall i = 2, \dots, m \exists n_i : \alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1}) \end{cases}$$

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:

$$\begin{aligned} \alpha_1^{n_1} &= a_1 \in F \Leftrightarrow \alpha_1 = \sqrt[n_1]{a_1} \\ F &\preceq F(\alpha_1) \\ \alpha_2^{n_2} &= a_2 \in F(\alpha_1) \Leftrightarrow \alpha_2 = \sqrt[n_2]{a_2} \\ F &\preceq F(\alpha_1, \alpha_2) \\ &\dots \end{aligned}$$

Theorem 7.22. *di Galois.*

Sia

1. $f(x) \in F[x]$, $\text{ch}F = 0$
2. $K = CS(f(x), F)$

allora

$$f(x) \text{ e' risolubile per radicali} \Leftrightarrow \mathcal{G}(K, F) \text{ e' risolubile}$$

8 *

Index

Campi chiusi e chiusura, 15
Campi di spezzamento, 13
Campi finiti, 16
campo chiuso, 15
campo coniugato, 29
campo di spezzamento, 13
Caratteristica, 4
caratteristica, 4
catena risolvibile, 33
chiusura, 15
Ciclotomia, 32
corrispondenza di Galois, 27

elemento

algebrico, 9
trascendente, 9

estensione

di Galois, 27
finita, 6
finitamente generata, 8
normale, 23
semplice, 8
separabile, 17

Estensione di Campi, 3

Estensioni, 6

Estensioni ciclotomiche, 30

Estensioni normali, 23

Estensioni separabili, 17

formule di Viete', 22

Gruppi risolubili, 33

Gruppo di Galois, 24

gruppo di Galois, 24

gruppo transitivo, 28

leading term, 21

ordinamento lessicografico, 21

Polinomi simmetrici, 20

polinomio derivato, 2

polinomio minimo, 9

Preliminari, 1

Riga e compasso, 31

Risolubilita' di S_n , 34

sottocampo fondamentale, 5

Teorema fondamentale dell'algebra, 29

Zorn lemma, 3