

# COMPLEMENTI

Note Title

20/12/2018

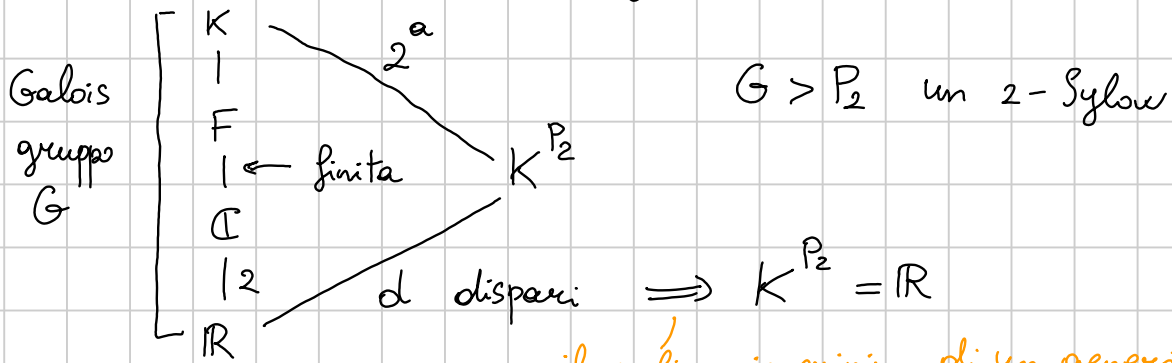
## Teorema fondam. dell'algebra

- $f(x) \in \mathbb{R}[x]$  deg  $f(x) \geq 3$  dispari  $\Rightarrow f(x)$  riducibile
  - $\mathbb{C}$  non haestens. quadratiche  
 $x^2 + ax + b = 0$
- teorema dei valori intermedi,  
primo input analitico*

$$\mathbb{C} \ni \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

*in  $\mathbb{C}$  riesco ad estrarre radici quadrate*

- Per assurdo  $\mathbb{C}$  non alg. chiuso



*il polinomio minimo di un generatore ha grado dispari, quindi e' di grado 1 (deve essere irriducibile)*

L'unica ext. quadratica di  $\mathbb{R}$  e'  $\mathbb{C}$

$$\frac{\mathbb{R}[x]}{(x^2 + ax + b)} \simeq \mathbb{C}$$

$$P_2 > H_m > H_{m-1} > \dots > H_0 = \{e\}$$

└───┬───┘  
2    2

Via teoria di Galois otteniamo una catena di estensioni

$$K >_2 K^{H_1} >_2 K^{H_2} > \dots > K^{H_m} >_2 K^{P_2} = \mathbb{R}$$

Da  $\mathbb{C}$  a  $K$  si passa con ext quadratiche  $\Rightarrow K = \mathbb{C}$

# Il teorema delle funzioni simmetriche

$$a+b+c$$

$$a^2b + b^2c + c^2a + ab^2 + bc^2 + ca^2$$

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \quad \forall \sigma \in S_n$$

Esempi  $\cdot X_1^k + \dots + X_n^k$

- funzioni simm. elementari

$$a+b+c, \quad ab+bc+ca, \quad abc$$

$$e_i = \sum_{\substack{|I|=i \\ I \subseteq \{1, \dots, n\}}} \prod_{j \in I} x_j$$

In 4 variabili,  $a+b+c+d = e_1$

$$ab+ac+ad+bc+bd+cd = e_2$$

$$abc+abd+acd+bcd = e_3$$

$$abcd = e_4$$

$$(x-x_1) \dots (x-x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \dots + (-1)^n e_n$$

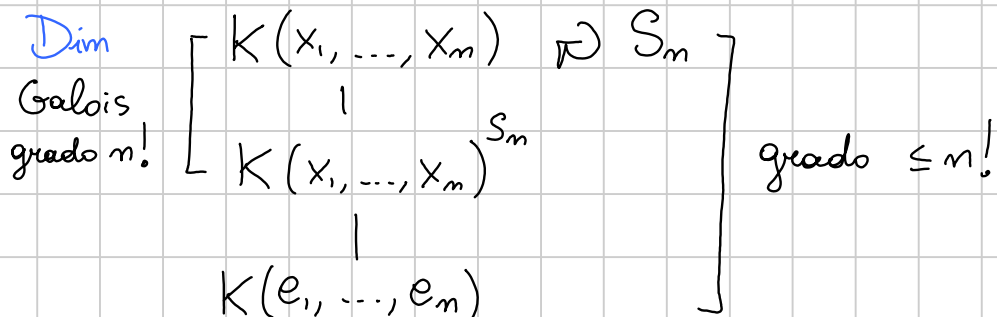
Teo Sia  $f(x_1, \dots, x_n) \in K(x_1, \dots, x_n)$  simmetrica

$$\exists g \in K(e_1, \dots, e_n) \text{ t.c. } f(x_1, \dots, x_n) = g(e_1, \dots, e_n)$$

Esempio  $a^2b + a^2c + \dots + cb^2 = (a+b+c)(ab+bc+ca)$

$$- 3abc$$

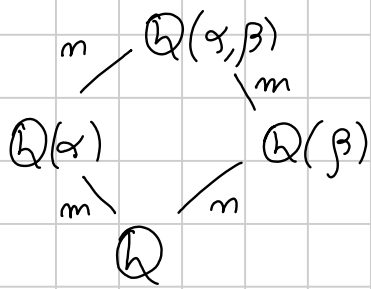
$$= e_1 e_2 - 3e_3$$



$$(t-x_1) \dots (t-x_m) = t^n - e_{n-1} t^{n-1} + \dots \pm e_n t^m$$

Siccome  $K(x_1, \dots, x_n)$  = campo di spezzamento  
del polinomio qui sopra,  
ottengo  $[K(x_1, \dots, x_m) : K(e_1, \dots, e_n)] \leq (\deg)! = n!$

$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$  se  $\deg(\alpha), \deg \beta$  coprimi



$\alpha_1, \dots, \alpha_m$  = coniugati di  $\alpha$

$\beta_1, \dots, \beta_m$  = \_\_\_\_\_  $\beta$

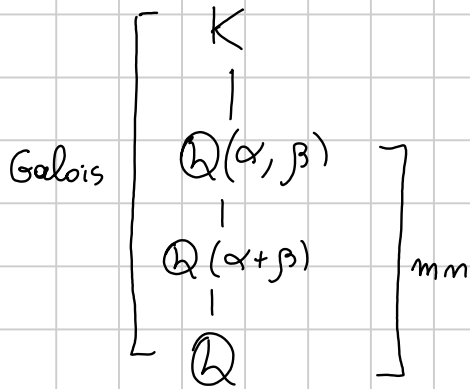
"lessicografico"

Oss Su  $\mathbb{C}$  c'è un ordinamento compatibile con la somma:

$$a_1 + ib_1 < a_2 + ib_2 \iff \begin{cases} \sigma & a_1 < a_2 \\ \sigma & a_1 = a_2 \text{ e } b_1 < b_2 \end{cases}$$
$$a_3 + ib_3 \leq a_4 + ib_4$$

Consideriamo l'insieme finito  $\{ \alpha_i + \beta_j \mid \substack{i=1, \dots, m \\ j=1, \dots, n} \}$

Diciamo che il massimo di questo insieme sia  $\alpha_k + \beta_l$ ,  
dove  $a_k = \max \{ \alpha_i \}, \beta_l = \max \{ \beta_j \}$



Le radici del polinomio minimo di  $\alpha + \beta$  sono i  $\sigma(\alpha + \beta)$  al variare di  $\sigma \in \text{Gal}(K/\mathbb{Q})$   
alcuni degli  $\alpha_i + \beta_j$

Certamente  $\forall i \forall j$  trovo  $\sigma$  t.c.  $\sigma(\alpha) = \alpha_i$   
L ci sono  $m \cdot n$  omomorfismi  $\neq 0$   $\sigma(\beta) = \beta_j$   
di  $\mathbb{Q}(\alpha, \beta)$  in  $\mathbb{C}$

(questo dipende da  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\beta) : \mathbb{Q}]$ )

Osserviamo che  $\sigma(\alpha_k + \beta_l) = \alpha_i + \beta_j$  e per

$\sigma \neq \text{id}$  se avessi  $\alpha_i + \beta_j = \alpha_k + \beta_l \geq \alpha_i + \beta_j$

otterrei un assurdo.

$\Rightarrow \alpha_k + \beta_l$  non è fissato da alcun  $\sigma$

$$\Rightarrow [\mathbb{Q}(\alpha_k + \beta_l) : \mathbb{Q}] = m \cdot n$$

$$\Rightarrow [\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = mn$$

Rivediamo i punti chiave della dimostrazione:

① Il max di  $\alpha_i + \beta_j$  è  $\max \{\alpha_i\} + \max \{\beta_j\}$ , questo garantisce  $\sigma(\alpha_k + \beta_l) \neq \alpha_k + \beta_l$  se  $\sigma \neq \text{id}$ , perché se  $\sigma \neq \text{id}$  allora o  $\sigma(\alpha_k) < \alpha_k$  o  $\sigma(\beta_l) < \beta_l$ , o entrambi, e quindi  $\sigma(\alpha_k) + \sigma(\beta_l) < \alpha_k + \beta_l$

②  $\sigma(\alpha_k + \beta_l) \neq \tau(\alpha_k + \beta_l)$  se  $\sigma \neq \tau$ , perché se fossero uguali otterrei:  $\tau^{-1}\sigma(\alpha_k + \beta_l) = \alpha_k + \beta_l$ , quindi  $\tau^{-1}\sigma = \text{id} \Rightarrow \tau = \sigma$ .

③ I coniugati di  $\alpha_k + \beta_l$  sono TUTTI (e soli) gli  $\alpha_i + \beta_j$  (perché ogni  $\sigma$  produce un coniug. diverso)

④ Questo implica  $[\mathbb{Q}(\alpha_k + \beta_l) : \mathbb{Q}] = mn$  ed inoltre

$$[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha_k + \beta_l) : \mathbb{Q}], \text{ perché}$$

$\alpha + \beta$  e  $\alpha_k + \beta_l$  coniugati, quindi hanno lo stesso grado su  $\mathbb{Q}$ .

⑤ Ne segue  $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = mn = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ ,

che combinato con  $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$  dà

l'uguaglianza voluta

# Teorema della progressione aritmetica di Dirichlet

$$a, b \in \mathbb{Z} \quad \text{con} \quad (a, b) = 1 \quad a \neq 0$$

Allora l'insieme  $\{ma+b, m \in \mathbb{Z}\}$  contiene infiniti numeri primi

Dim per  $b=1$

$$\text{Supponiamo } p \text{ primo, } c \text{ intero, } \begin{cases} c^a \equiv 1 \pmod{p} \\ c^k \not\equiv 1 \pmod{p} \quad 0 < k < a \end{cases}$$

$$\Rightarrow \text{ord}_p(c) = a \Rightarrow a \mid p-1$$

Mi basta dim che  $\exists$  infiniti  $p$  per cui esiste  $c$  di ordine esattamente  $a$

$$\text{Considero } x^a - 1 = \prod_{x|a} \Phi_x(x), \text{ dove } \Phi_x \text{ e' il}$$

polin. minimo delle radici  $x$ -esime di 1

$$(a = \sum_{x|a} \deg \Phi_x)$$

Cerco radici di  $\Phi_a(x)$  che non siano radici di  $\prod_{k < a} (x^k - 1) =: q(x)$

$$(\Phi_a(x), q(x)) = 1 \Rightarrow \overset{\mathbb{Q}[x]}{\cup} \Phi_a(x) u(x) + \overset{\mathbb{Q}[x]}{\cup} q(x)v(x) = 1$$

$$\Rightarrow \underset{\mathbb{Z}[x]}{\cup} \Phi_a \cdot \underset{\mathbb{Z}[x]}{\cup} U + q(x) \cdot \underset{\mathbb{Z}[x]}{\cup} V(x) = A \in \mathbb{Z}$$

Esistono infiniti primi modulo i quali  $\Phi_a(x)$  abbia una radice, chiamiamola  $c$

$$\overbrace{\Phi_a(c)}^0 \cdot U(c) + q(c) V(c) \equiv A \pmod{p}$$

se  $p \nmid A$ , allora  $p \nmid q(c)$

Riassumendo: • esistono infinite coppie  $(p, c \bmod p)$  t.c.

$$\Phi_a(c) \equiv 0 \pmod p$$

• la congruenza qui sopra implica che per ogni tale coppia si abbia  $q(c) \nmid \Phi_a(c) \pmod p$

• Scartando i  $p$  che dividono  $A$ , ho ancora  $\infty$  coppie t.c.  $\Phi_a(c) \equiv 0 \pmod p, q(c) \not\equiv 0 \pmod p$

•  $c^a \equiv 1 \pmod p$ : infatti  $x^a - 1 = \Phi_a(x) \cdot s(x)$

$$\Rightarrow c^a - 1 \equiv \Phi_a(c) s(c) \equiv 0 \pmod p$$

e d'altro canto  $0 \neq q(c) = \prod_{k < a} (c^k - 1) \pmod p$

$\Rightarrow$  FINE!

□

Esempio

$$3k+1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$q(x) = x - 1 \quad (x^2 + x + 1) - (x - 1) \cdot (x + 2) = 3 = A$$

Quindi devo scartare il primo 3, e poi voglio primi modulo i quali  $\Phi_3$  abbia radici. Il modo più semplice è quello di guardare i fattori primi di  $\Phi_3(n)$  al variare di  $n \in \mathbb{Z}$ .

da scartare



$$\Phi_3(2) = 7 \equiv 1 \pmod 3, \quad \Phi_3(3) = 13 \equiv 1 \pmod 3, \quad \Phi_3(4) = 21 = 3 \cdot 7$$

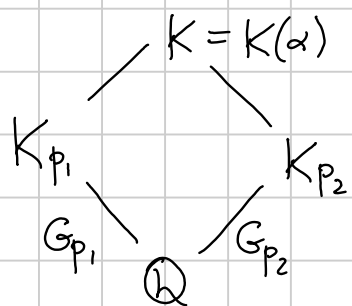
$$\Phi_3(5) = 31 \equiv 1 \pmod 3, \quad \Phi_3(6) = 43 \equiv 1 \pmod 3, \quad \dots$$

## Problema inverso di Galois per gruppi abeliani

$$G \simeq G_{p_1} \times \dots \times G_{p_k} \quad \text{gruppo abeliano finito.}$$

Vorrei trovare un polinomio il cui campo di spezz. abbia gruppo di Galois  $G$ .

Basta realizzare  $G_{p_1}, G_{p_2}, \dots, G_{p_k}$ :



$$\text{Gal}(K/\mathbb{Q}) \hookrightarrow G_{p_1} \times G_{p_2}$$

$$\begin{aligned} & \downarrow \\ \text{cardinalità} \quad [K:\mathbb{Q}] &= [K_{p_1}:\mathbb{Q}] \cdot \\ & [K_{p_2}:\mathbb{Q}] \\ &= \#G_{p_1} \cdot \#G_{p_2} \end{aligned}$$

Basta prendere il polin. minimo di  $\alpha$ .

Ci siamo così ridotti al caso  $G = p$ -gruppo.

$$\text{Studiamo } G_p = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$$

Cominciamo a realizzare  $\mathbb{Z}/p^{a_1}\mathbb{Z}$ .

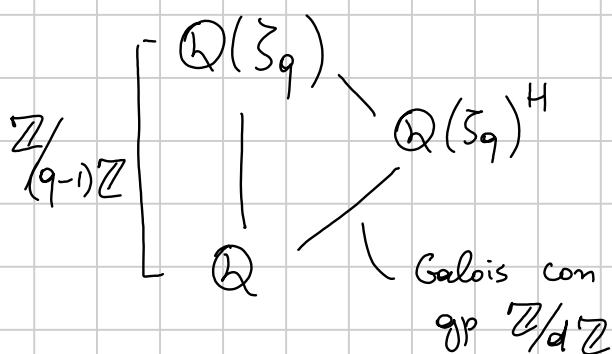
Esempio:  $\mathbb{Z}/4\mathbb{Z}$

$$\mathbb{Z}/12\mathbb{Z} \left[ \begin{array}{c} \mathbb{Q}(\zeta_{13}) \\ | \\ \mathbb{Q} \end{array} \right] \begin{array}{c} \backslash \\ \mathbb{Q}(\zeta_{13})^H \\ \hline \mathbb{Q} \end{array} \begin{array}{c} |H|=3 \\ \hline \text{gp di Galois} \end{array} \quad \mathbb{Z}/12\mathbb{Z} / H \simeq \mathbb{Z}/4\mathbb{Z}$$

Notare che  $H \triangleleft \mathbb{Z}/12\mathbb{Z}$ !



In generale: realizzare  $\mathbb{Z}/d\mathbb{Z}$



Sia  $d$  un divisore di  $q-1$ .  
 $\mathbb{Z}/(q-1)\mathbb{Z}$  c'è un sottogruppo di indice  $d$ , chiamiamolo  $H$ , ovviamente normale

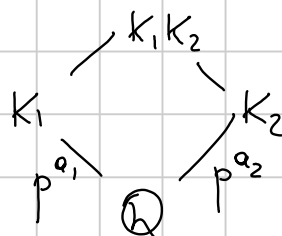
Realizzare  $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$

Per ogni  $\mathbb{Z}/p^{a_i}\mathbb{Z}$  scegliamo un primo  $q_i \equiv 1 \pmod{p^{a_i}}$

e dentro  $\mathbb{Q}(\zeta_{q_i})$  prendiamo il sottocampo che abbia grado  $p^{a_i}$  su  $\mathbb{Q}$ , chiamiamolo  $K_i$

$$K := K_1 \dots K_n \quad \text{Gal}(K/\mathbb{Q}) \hookrightarrow \prod \text{Gal}(K_i/\mathbb{Q})$$

ed inoltre si ha



$$[K_1, K_2 : \mathbb{Q}] = [K_1, K_2 : K_2] [K_2 : \mathbb{Q}]$$

$$= [K_1 : K_1 \cap K_2] [K_2 : \mathbb{Q}]$$

$$\hookrightarrow \text{è } \mathbb{Q}? \text{ Sì, } \subseteq \mathbb{Q}(\zeta_{q_1}) \cap \mathbb{Q}(\zeta_{q_2}) = \mathbb{Q}$$

$$= [K_1 : \mathbb{Q}] [K_2 : \mathbb{Q}].$$

Ne segue (per induz. su  $n$ ) che  $[K_1 \dots K_n : \mathbb{Q}] =$

$$= [K_1 : \mathbb{Q}] \dots [K_n : \mathbb{Q}] = \#\text{Gal}(K_1/\mathbb{Q}) \dots \#\text{Gal}(K_n/\mathbb{Q})$$

e quindi  $\text{Gal}(K/\mathbb{Q}) \hookrightarrow \prod_{i=1}^n \text{Gal}(K_i/\mathbb{Q})$  è un

isomorfismo per questioni di cardinalità.