Appello I, ALGEBRA 8/2/2012 SOLUZIONI

② (a) F crc. di $f = x^3 - 7$ su $\mathbb{Q}$

- zeri di f: $\sqrt[3]{7}$, $\alpha\sqrt[3]{7}$, $\alpha^2\sqrt[3]{7}$, dove $\alpha = -\frac{1}{2} + i\,\frac{1}{2}\sqrt{3}$
- $F = \mathbb{Q}(\alpha, \sqrt[3]{7})$ con $[F:\mathbb{Q}] = 6$
- $\mathbb{Q}$-base di F: $\{1, \alpha, \sqrt[3]{7}, \alpha\sqrt[3]{7}, (\sqrt[3]{7})^2, \alpha(\sqrt[3]{7})^2\}$

(infatti $\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7})}_{\text{grado } 3} \subset F$)

grado 3 con base $\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2\}$

grado 2: x^2+x+1 è polinomio minimo di α su $\mathbb{Q}(\sqrt[3]{7})$ quindi base $\{1,\alpha\}$

- $\mathbb{Q} \subset F$ estensione di Galois poiché crc. di f separabile

Pertanto $G \cong G' \leq S_3$, $|G| = [F:\mathbb{Q}] = 6$ e quindi $G \cong S_3$

(b) Gli elementi di G sono determinati da $\varphi(\alpha)$ e $\varphi(\sqrt[3]{7})$.

- Poiché $\varphi(\alpha)^3 = 1$ e $\varphi(\sqrt[3]{7})^3 = 7$

sappiamo

$\varphi(\alpha) \in \{\alpha, \alpha^2\}$ e $\varphi(\sqrt[3]{7}) \in \{\sqrt[3]{7}, \alpha\sqrt[3]{7}, \alpha^2\sqrt[3]{7}\}$

- Abbiamo quindi

φ	$\varphi(\alpha)$	$\varphi(\sqrt[3]{7})$	ord φ
$id_F = \varphi_1$	α	$\sqrt[3]{7}$	1
φ_2	α	$\alpha\sqrt[3]{7}$	3 (vedi sotto)
φ_3	α	$\alpha^2\sqrt[3]{7}$	3
φ_4	α^2	$\sqrt[3]{7}$	2
φ_5	α^2	$\alpha\sqrt[3]{7}$	2
φ_6	α^2	$\alpha^2\sqrt[3]{7}$	2

- L'ordine di φ_2:

$$\sqrt[3]{7} \xmapsto{\varphi_2} \alpha\sqrt[3]{7} \xmapsto{\varphi_2} \alpha^2\sqrt[3]{7} \xmapsto{\varphi_2} \alpha^3\sqrt[3]{7} = \sqrt[3]{7}$$

quindi $\varphi_2^{\,2}(\sqrt[3]{7}) \neq \sqrt[3]{7}$ e $\varphi_2^{\,2} \neq id_F$,

mentre $\varphi_2^{\,3}(\sqrt[3]{7}) = \sqrt[3]{7}$ e $\varphi_2^{\,3}(\alpha) = \alpha$, quindi $\varphi_2^{\,3} = id_F$.

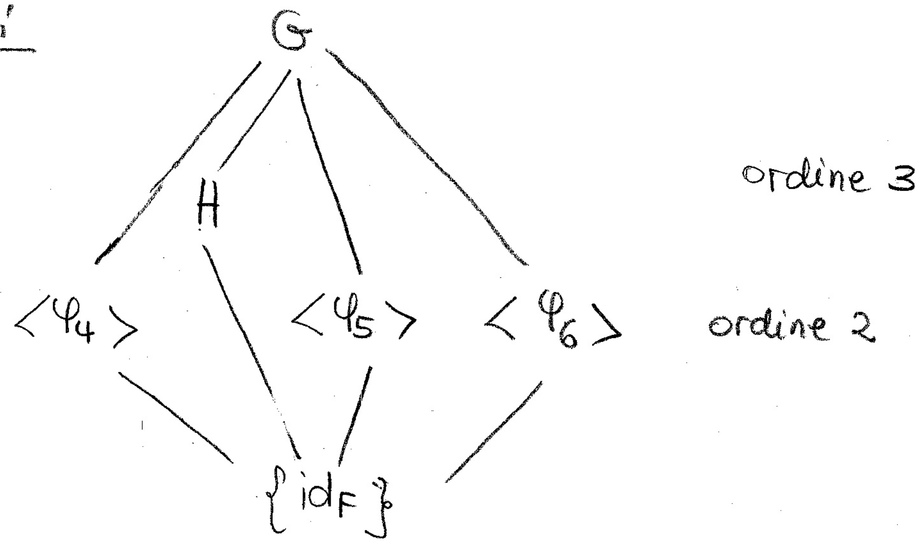
Analogamente si calcolano gli altri ordini.

(c) - I sottogruppi propri sono di ordine 2 o 3, quindi ciclici.
- Notiamo che $\varphi_2^{\,2}(\alpha) = \alpha$ e $\varphi_2^{\,2}(\sqrt[3]{7}) = \alpha^2\sqrt[3]{7}$,

quindi $\varphi_2^{\,2} = \varphi_3$ e $\varphi_3^{\,2} = \varphi_2^{\,4} = \varphi_2$. Dunque

$$H = \langle \varphi_2 \rangle = \{1, \varphi_2, \varphi_3\} = \langle \varphi_3 \rangle$$ unico sottogruppo di ordine 3

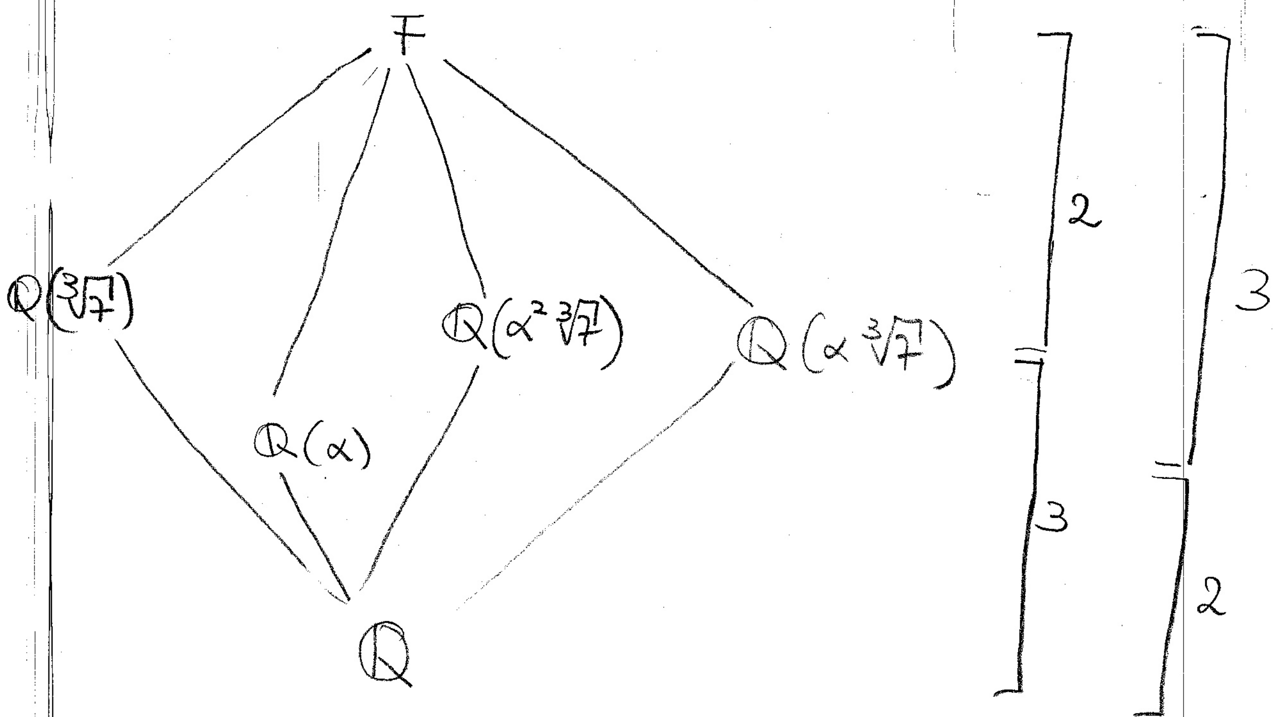
- <u>Sottogruppi</u>



- <u>Campi intermedi</u>

Si ha
$$Fix_F(H) = \mathbb{Q}(\alpha)$$
$$Fix_F\langle\varphi_4\rangle = \mathbb{Q}(\sqrt[3]{7})$$
$$Fix_F\langle\varphi_5\rangle = \mathbb{Q}(\alpha^2\sqrt[3]{7})$$
$$Fix_F\langle\varphi_6\rangle = \mathbb{Q}(\alpha\sqrt[3]{7})$$

Dunque si ha applicando il Teorema Fondamentale



(d) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7}) \subset F$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7})$: è di Galois se e solo se $\langle \varphi_4 \rangle \lhd G$

$\mathbb{Q}(\sqrt[3]{7}) \subset F$: gruppo di Galois $\langle \varphi_4 \rangle$

<u>Ma</u> $\langle \varphi_4 \rangle$ <u>non</u> è un sottogruppo normale: infatti

$$\varphi_5 \varphi_4 \varphi_5 \notin \langle \varphi_4 \rangle = \{ id_F, \varphi_4 \}$$

poiché $\varphi_5 \varphi_4 \varphi_5 (\sqrt[3]{7}) = \alpha^2 \sqrt[3]{7}$

Quindi

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7})$ non è un'estensione di Galois.

③ (a) Per ipotesi f ha gli zeri

$$\alpha \in \mathbb{R}, \quad \beta, \bar{\beta} \in \mathbb{C} \setminus \mathbb{R}$$

Quindi se E è crc. di f su $\mathbb{Q}$, si ha

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\alpha)}_{\substack{\text{grado } 3 \\ \text{poiché } f \text{ è} \\ \text{polinomio minimo} \\ \text{di } \alpha \text{ su } \mathbb{Q}}} \underbrace{\subsetneq}_{\text{grado } \geq 2} E$$

Pertanto $6 \leq [E : \mathbb{Q}] \leq 6 = 3!$

e $|G| = [E : \mathbb{Q}] = 6$

Poiché G è isomorfo a un sottogruppo di S_3 e $|S_3| = 6$, deduciamo $G \cong S_3$.

(b) $F = K[x]/(f) \cong K(\alpha)$ è un'estensione di K di grado $\deg f = d$, quindi $|F| < \infty$.

Per 15.2 sappiamo che $K \subset F$ è un'estensione di Galois (poiché $P \subset K \subset F$ e $P \subset F$ è di Galois). In particolare, $K \subset F$ è un' estensione normale. Dunque f, essendo il polinomio minimo di α su K (a meno di costante), è prodotto di fattori lineari in $F[x]$. Dunque F è crc. di f su K,

(2) (a) F crc. di $f = x^4 - 9$ su $\mathbb{Q}$

- zeri di f: $\sqrt{3}$, $-\sqrt{3}$, $i\sqrt{3}$, $-i\sqrt{3}$
- $F = \mathbb{Q}(i, \sqrt{3})$ con $[F : \mathbb{Q}] = 4$
- $\mathbb{Q}$ - base di F : $\{1, i, \sqrt{3}, i\sqrt{3}\}$
- $\mathbb{Q} \subset F$ estensione di Galois poiché crc. di f separabile

(b) Gli elementi di G sono determinati da $\varphi(i)$ e $\varphi(\sqrt{3})$.

- poiché $\varphi(i)^2 = -1$ e $\varphi(\sqrt{3})^2 = 3$ sappiamo $\varphi(i) \in \{i, -i\}$ e $\varphi(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$
- Abbiamo quindi

φ	$\varphi(i)$	$\varphi(\sqrt{3})$	ord φ
$id_F = \varphi_1$	i	$\sqrt{3}$	1
φ_2	i	$-\sqrt{3}$	2
φ_3	$-i$	$\sqrt{3}$	2
φ_4	$-i$	$-\sqrt{3}$	2

da cui segue che G è isomorfo al gruppo di Klein.

(c) I sottogruppi propri sono tutti ciclici di ordine 2

$$\begin{tikzcd}
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \varphi_2 \rangle \arrow[dr, dash] & \langle \varphi_3 \rangle \arrow[d, dash] & \langle \varphi_4 \rangle \arrow[dl, dash] \\
 & \{id_F\} &
\end{tikzcd}$$

con $\quad Fix_F \langle \varphi_2 \rangle = \mathbb{Q}(i)$

$Fix_F \langle \varphi_3 \rangle = \mathbb{Q}(\sqrt{3})$

$Fix_F \langle \varphi_4 \rangle = \mathbb{Q}(i\sqrt{3})$

quindi applicando il Teorema Fondamentale

i campi intermedi

$$\begin{tikzcd}
 & F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(i\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(d) $\underbrace{\mathbb{Q} \subset L}_{\text{di Galois}} \subset F$

sse $Gal(F/L) \lhd G$

Poiché G è abeliano, tutti i sottogruppi sono normali, quindi $\mathbb{Q} \subset L$ sempre di Galois.

(e) $Gal(F/\mathbb{Q}(\sqrt{3})) = Gal(F/Fix_F\langle\varphi_3\rangle) = \langle\varphi_3\rangle$.

3 (a) NO, poiché $x^4+x^2+1 = (x^2+x+1)^2$ non è irriducibile, quindi non si tratta di un campo

(b) sì, come nel primo appello, Es. 3 (b), si vede che $F = K[x]/(f)$ è crc, di f su K. Poiché $[F:K] = \deg f = d$, si ha $|F| = |K|^d = p^{nd}$

quindi $F \cong GF(p^{nd})$.