Lezione 18 - 5/06/19

martedì 30 aprile 2019 15:13

Esercizio 3

(i) α, β algebrici su $\mathbb{Q}$ di grado 2. $\alpha^2 \in \mathbb{Q}$, $\beta^2 \in \mathbb{Q}$

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) \iff \frac{\alpha}{\beta} \in \mathbb{Q}$$

$\boxed{\Leftarrow}$ $\alpha = q\beta$ con $q \in \mathbb{Q}$ $\Rightarrow$ $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$ e per grado ho l'uguaglianza

$\boxed{\Rightarrow}$ $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ $\quad \subseteq$

$$a + b\beta = \alpha \quad \text{con } a, b \neq 0$$

Elevo al quadrato

$$a^2 + 2ab\beta + b^2\beta^2 = \alpha^2 \iff \beta = \frac{\alpha^2 - b^2\beta^2 - a^2}{2ab}$$

$\alpha^2, \beta^2 \in \mathbb{Q}$ per ipotesi $\Rightarrow \beta \in \mathbb{Q}$ assurdo

Ma allora a e b non possono essere entrambi $\neq 0$.

1) Se $b = 0$ Assurdo perché $\alpha = a$, ma $a \in \mathbb{Q}$

2) $a = 0$ e deve essere vero per forza perché è l'ultimo caso rimasto.

$\hookrightarrow$ $b\beta = \alpha$ cioè $\frac{\alpha}{\beta} = b \in \mathbb{Q}$

(ii) $p_1, \ldots, p_n$ primi distinti su $\mathbb{Z}$. Grado e Gal di $\mathbb{E}_n \supseteq \mathbb{Q}$ con

$$\mathbb{E}_n = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$$

Claim: Grado $= 2^n$ $\quad Gal(\mathbb{E}_n/\mathbb{Q}) = (\mathbb{Z}/2)^n$

Per induzione su n.

$\boxed{n=1}$ funziona $\mathbb{Q}(\sqrt{p_1}) \supseteq \mathbb{Q}$ $\quad x^2 - p_1$ irr. grado 2 $\Rightarrow \mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$ Galois e tutto bello insomma

$\boxed{n \Rightarrow n+1}$ Vogliamo dimostrare che $[\mathbb{E}_{n+1} : \mathbb{Q}] = 2^{n+1}$

Per dirlo è sufficiente dire che $[\mathbb{E}_{n+1} : \mathbb{E}_n]$ ha grado 2 e questa ha grado 2 se l'estensione

$$\begin{array}{ccc} & \mathbb{E}_{n+1} & \\ \mathbb{E}_n & & \mathbb{Q}(\sqrt{p_{n+1}}) \end{array}$$

$$\begin{array}{ccc} \mathbb{E}_n & & \mathbb{Q}(\sqrt{p_{n+1}}) \\ & \mathbb{E}_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) & \\ 2^n & \mid & 2 \\ & \mathbb{Q} & \end{array}$$

grado 2 e questa ha grado 2 se l'estensione

$$\mathbb{Q}(\sqrt{p_{n+1}}) \,/\, \mathbb{Q}(\sqrt{p_{n+1}}) \cap \mathbb{E}_n$$

ha grado 2. Per dimostrarlo mi basta dire che

$$\mathbb{E}_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$$

Dimostriamolo:

$\mathbb{E}_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) \subseteq \mathbb{Q}(\sqrt{p_{n+1}})$ e quindi ha grado 1 o 2

$\mathbb{Q}(\sqrt{p_{n+1}})$ $\qquad$ $\mathbb{Q}$

Voglio escluderlo

Se $\mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{E}_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) \Rightarrow \mathbb{Q}(\sqrt{p_{n+1}})$ è sottoestensione anche di $\mathbb{E}_n$

Ma le sottoest. di $\mathbb{E}_n$ le conosco tutte:

Per ip induttiva $Gal(\mathbb{E}_n/\mathbb{Q}) \cong (\mathbb{Z}/2)^n$. Le sottoest. di grado 2 sono quindi in bigezione con i sottogr. normali di indice 2. Sono esattamente $2^n - 1$

$$(\mathbb{Z}/2)^n \longrightarrow \mathbb{Z}/2$$

di contro io conosco 2^n-1 est. di grado 2 contenute lì dentro: sono tutti i possibili prodotti di $\sqrt{p_i}$

$\sqrt{p_1}$ - - - - $\sqrt{p_n}$

che in totale sono $2^n - 1$ e sono tutte distinte per il punto (i).

$\sqrt{p_1}$ $\sqrt{p_2}$ $\sqrt{p_3}$

$\sqrt{p_1p_2}$ $\sqrt{p_1p_3}$ $\sqrt{p_2p_3}$

$\sqrt{p_1p_2p_3}$

$n=3$

$7 = 2^3 - 1$

Se adesso confronto $\mathbb{Q}(\sqrt{p_{n+1}})$ con una a caso di queste est. di grado 2, scopro che sono distinte perché il rapporto contiene $\sqrt{p_{n+1}}$ da qualche parte che $\notin \mathbb{Q}$.

$$\begin{array}{ccc} & \mathbb{E}_{n+1} & \\ 2 & & \\ \mathbb{E}_n & & \mathbb{Q}(\sqrt{p_{n+1}}) \\ (\mathbb{Z}/2)^n & \mathbb{Q} & \mathbb{Z}/2 \end{array}$$

Per teorema Galois vale che

$$Gal(\mathbb{E}_{n+1}/\mathbb{Q}) = (\mathbb{Z}/2)^n \times \mathbb{Z}/2 = (\mathbb{Z}/2)^{n+1}$$

$\mathbb{K}_n$ $\qquad$ $\mathbb{Q}(\sqrt{p_{n+1}})$ $\qquad$ $Gal(\ /\mathbb{Q}) = (\mathbb{Z}/2) \times \mathbb{Z}/2 \times \mathbb{Z}/2)$

$(\mathbb{Z}/2)^n$ $\quad \mathbb{Q} \quad$ $\mathbb{Z}/2$

(iii) γ, δ di grado 3 $\quad \gamma^3 \in \mathbb{Q}$, $\delta^3 \in \mathbb{Q}$ $\quad \mathbb{Q}(\gamma) = \mathbb{Q}(\delta) \Leftrightarrow \frac{\gamma}{\delta} \in \mathbb{Q}$ o $\frac{\gamma}{\delta^2} \in \mathbb{Q}$

$\boxed{\Leftarrow}$ $\frac{\gamma}{\delta} \in \mathbb{Q} \Rightarrow \frac{\gamma}{\delta} = q \quad \gamma = q\delta$ tesi

$\frac{\gamma}{\delta^2} \in \mathbb{Q} \Rightarrow \gamma = q\delta^2 \quad \gamma \in \mathbb{Q}(\delta^2)$ ma $\mathbb{Q}(\delta^2) = \mathbb{Q}(\delta)$ in quanto

$\delta^2 \cdot \delta^2 = \delta^3 \cdot \delta$ e $\delta^3 \in \mathbb{Q}$ dunque $\mathbb{Q}(\delta) \subseteq \mathbb{Q}(\delta^2)$

$\supseteq$ ovvio

$\Rightarrow \gamma \in \mathbb{Q}(\delta)$

$\boxed{\Rightarrow}$ $\mathbb{Q}(\gamma) = \mathbb{Q}(\delta) \quad \exists a, b, c \in \mathbb{Q} \setminus \{0\}$ t.c.

$a + b\gamma + c\gamma^2 = \delta$ $\quad$ elevo al cubo

$a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + a_4\gamma^4 + a_5\gamma^5 + a_6\gamma^6 = \delta^3$

$a_0 + \underbrace{(a_1 + a_4\gamma^3)}_{\in \mathbb{Q}}\gamma + \underbrace{(a_2 + a_5\gamma^3)}_{\in \mathbb{Q}}\gamma^2 + \underbrace{\gamma^3(a_3 + a_6\gamma^3)}_{\in \mathbb{Q}} = \underbrace{\delta^3}_{\in \mathbb{Q}}$ $\qquad$ $\gamma^3 \in \mathbb{Q}$, $\delta^3 \in \mathbb{Q}$

Ma allora γ annulla un polinomio di grado 2 su $\mathbb{Q}$ e questo è assurdo

- Tutti e tre $\neq 0$ No
- se solo 1 dei 3 uguale a 0 succede una cosa analoga
- Se 2 dei 3 uguali a 0 così:

$b, c = 0 \Rightarrow \delta = a \in \mathbb{Q}$ $\lightning$

$a, c = 0 \quad \frac{\delta}{\gamma} \in \mathbb{Q}$:)

$a, b = 0 \quad \frac{\delta}{\gamma^2} \in \mathbb{Q}$:)

(iv) $p_1 \_\_ p_n$ in $\mathbb{Z}$ primi distinti $\quad \mathbb{L}_n = \mathbb{Q}(\sqrt[3]{p_1}, \_\_, \sqrt[3]{p_n}, \zeta_3)$

$[\mathbb{L}_n : \mathbb{Q}]$ e $Gal(\mathbb{L}_n/\mathbb{Q})$

Claim: $3^n \cdot 2$ grado

$\sqrt{p_i} \xrightarrow[id]{} \sqrt{p_i}\,\zeta_3 \qquad \zeta_3 \to \zeta_3^{-1}$

$(\mathbb{Z}/3 \times \_\_ \times \mathbb{Z}/3) \rtimes \mathbb{Z}/2$

Per induzione su n : Grado $= 3^n \cdot 2$ $\quad Gal(L_n/\mathbb{Q}) = (\mathbb{Z}/3)^n \rtimes \mathbb{Z}/2$ $\quad \varphi: \mathbb{Z}/2 \longrightarrow Aut((\mathbb{Z}/3)^n)$

$1 \longmapsto \begin{pmatrix} 2 & & \\ & 2 & \\ & & \ddots & \\ & & & 2 \end{pmatrix}$

$\sqrt[3]{2} \quad \sqrt[3]{3} \quad \zeta_3$

$\sigma_1 : \begin{array}{l} \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\,\zeta_3 \\ \sqrt[3]{3} \longrightarrow \sqrt[3]{3} \\ \zeta_3 \longrightarrow \zeta_3 \end{array} \qquad \sigma_2 : \begin{array}{l} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ \sqrt[3]{3} \longrightarrow \sqrt[3]{3}\,\zeta_3 \\ \zeta_3 \longrightarrow \zeta_3 \end{array} \qquad \delta : \begin{array}{l} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ \sqrt[3]{3} \longrightarrow \sqrt[3]{3} \\ \zeta_3 \longrightarrow \zeta_3^{-1} \end{array}$

$\delta \sigma_1 \delta = \sigma_1^{-1} \qquad \delta \sigma_2 \delta = \sigma_2^{-1} \qquad\qquad \sigma_1 \sigma_2 = \sigma_2 \sigma_1$

$\langle \sigma_2 \rangle \cap \langle \sigma_1 \rangle = \{e\}$ tirano in ballo estensioni distinte (o si fa il conto)

$\langle \sigma_1 \rangle$ e $\langle \sigma_2 \rangle$ si norm. perché commutano

$\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \cong \mathbb{Z}/3 \times \mathbb{Z}/3$

$\langle \delta \rangle$ Normalizza $\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle$

$\langle \delta \rangle \cap (\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle) = \{e\}$ perché δ smuove ζ_3 e gli altri no.

$(\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle) \rtimes \langle \delta \rangle \cong (\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes_\varphi \mathbb{Z}/2$

Se so che $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \zeta_3) : \mathbb{Q}] = 3^2 \cdot 2$ ho finito

$(\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle) \rtimes \langle \delta \rangle \longrightarrow (\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes_\varphi \mathbb{Z}/2$

$\sigma_1 \longmapsto (1,0,0)$

$\sigma_2 \longmapsto (0,1,0)$

$\delta \longmapsto (0,0,1)$

$\varphi : \mathbb{Z}/2 \longrightarrow Aut(\mathbb{Z}/3 \times \mathbb{Z}/3)$

$1 \longmapsto \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

$\delta \sigma_1 \delta = \sigma_1^{-1}$

$(0,0,1)(1,0,0)(0,0,1) = (0,0,1)(1,0,1) = \left((0,0) + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1+1\right) =$

$(2,0,0)$

$(0,0,1)(1,1,0)(0,0,1) = (2,2,0)$

$\delta \sigma_1 \sigma_2 \delta$

$\delta \sigma_1 \delta\, \delta \sigma_2 \delta = \sigma_1^{-1} \sigma_2^{-1}$

Claim: Grado $3^n \cdot 2$ $\quad Gal(L_n/\mathbb{Q}) = (\mathbb{Z}/3)^n \rtimes \mathbb{Z}/2$

$n=1$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{L}_1 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{p_1}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\sigma_1 : \begin{array}{l} \sqrt[3]{p_1} \longrightarrow \sqrt[3]{p_1}\,\zeta_3 \\ \zeta_3 \longrightarrow \zeta_3 \end{array} \qquad \delta : \begin{array}{l} \_\_\_ \\ \_\_\_ \end{array}$$

$$S_3 = (\mathbb{Z}/3) \rtimes_\varphi \mathbb{Z}/2$$

$$\varphi : \mathbb{Z}/2 \longrightarrow Aut(\mathbb{Z}/3)$$
$$1 \longmapsto (2)$$

$\boxed{n \Rightarrow n+1}$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{L}_{n+1} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{L}_n \arrow[dr, dash] \arrow[ddr, dash, "(\mathbb{Z}/3)^n \rtimes \mathbb{Z}_2"'] & & \mathbb{Q}(\sqrt[3]{p_{n+1}}) \arrow[dl, dash] \arrow[ddl, dash, "3"] \\
 & \cap \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Se dimostro che $\cap$ è $\mathbb{Q}$, allore il grado è a posto e posso pensare a def. il gruppo di Galois come ho fatto nell'esempio

$$\mathbb{Q}(\sqrt[3]{p_{n+1}}) \supseteq \cap$$

$$\cap \begin{array}{l} \nearrow \mathbb{Q} \\ \searrow \mathbb{Q}(\sqrt[3]{p_{n+1}}) \end{array} \longleftarrow \text{Voglio escluderti}$$

$\uparrow 3$

Stiamo cercando le sottoestensioni di grado 3 su $\mathbb{Q}$ di $\mathbb{L}_n$ che corrispondono ai sottogruppi di indice 3 in $(\mathbb{Z}/3)^n \rtimes \mathbb{Z}/2$

Sottoest. di grado 3:

$\boxed{\sqrt[3]{p_1} \quad \dots \quad \sqrt[3]{p_n}}$ — $\sqrt[3]{p_1}$ 0 1 2 $\qquad \sqrt[3]{p_1}\,\sqrt[3]{p_2}$

$\sqrt[3]{p_1}\,\zeta_3 \quad \dots \quad \sqrt[3]{p_n}\,\zeta_3 \qquad$ Ho 3 scelte $\forall$ primo $\qquad \sqrt[3]{p_1^2} \cdot \sqrt[3]{p_2^2}$

$\sqrt[3]{p_1}\,\zeta_3^2 \quad \dots \quad \sqrt[3]{p_n}\,\zeta_3^2$

$$\frac{3^n - 1}{2} \cdot 3$$

1 , 1 , 2

2 2 1

Queste ce l'ho. Se fossero tutte ho finito perché le confronto con $\mathbb{Q}(\sqrt[3]{p_{n+1}})$ e il rapporto NON appartiene a $\mathbb{Q}$ e dunque $\mathbb{Q}(\sqrt[3]{p_{n+1}}) \cap \mathbb{L}_n = \mathbb{Q}$

Per dire che sono tutte devo mostrare che ci sono ESATTAMENTE $\frac{3^n-1}{2} \cdot 3$ sott. di indice 3 in $(\mathbb{Z}/_3)^n \rtimes \mathbb{Z}_2$

$$(\mathbb{Z}/_3)^n \rtimes_\varphi \mathbb{Z}/_2 = G_n$$

<u>Oss 1</u>: gli elementi di G_n sono tutti di ordine 3 o 2

$$(\underbrace{1,0,1,0,1,1,1}, 1)(\underbrace{1,0,1,0,1,1,1}, 1) =$$

$$(\quad 0 \quad , 0)$$

<u>Oss 2</u>: Gruppi di indice 3 hanno $3^{n-1} \cdot 2$ elementi e di conseguenza contengono uno $(\mathbb{Z}/_3)^{n-1}$ al loro interno. Dunque tale sottogruppo contiene un iperpiano di $(\mathbb{Z}/_3)^n$

$$a_1 x_1 + \dots + a_n x_n = 0 \qquad a_i \in \mathbb{Z}/_3 \qquad \begin{matrix} x_1 + 2x_2 = 0 \\ 2x_1 + x_2 = 0 \end{matrix}$$

$$\frac{3^n - 1}{2}$$

<u>Oss 3</u>: Dato che ogni $(\mathbb{Z}/_3)^{n-1}$ è "uguale" agli altri a meno di Automorfismo, posso supporre che il mio iperpiano sia quello ident. delle prime n-1 coordinate

$$(\mathbb{Z}/_3 \times \dots \times \mathbb{Z}/_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}/_2$$

$$(\underbrace{\mathbb{Z}/_3 \times \dots \times \mathbb{Z}/_3}) \times 0$$

Voglio aggiungere el di ordine 2.

Dico che posso aggiungere (in modo che i gruppi finali sono distinti) l'el. di ordine 2 solo in 3 modi

$$(0 \_\_\_ 0, 0, 1) \leftarrow \qquad (1, 1, 0 \_\_\_ 0, 1)$$

$$(0 \_\_\_ 0, 1, 1) \leftarrow$$

$$(0 \_\_\_, 0, 2, 1) \leftarrow$$

$$\in (\mathbb{Z}_3)^{n-1}$$

$$(\underbrace{1,1,0 \_\_ 0}, 1)(\underbrace{1,1,0 \_\_ 0},0) = (0, \_\_ 0, 1)$$

$$\frac{3^n-1}{2} \cdot 3 \quad \text{sottogruppi di indice } 3$$

Definisco Gal come nell'esempio e ciaone

Esercizio 2: A N-nilpotente se $\exists a$ nilp $a \neq 0$ e se a nilp $\Rightarrow$ $a^N = 0$.

(i) A anello finito $\Rightarrow \mathcal{N} = \{\text{nilpotenti}\}$ è finito $a_1^{n_1} = 0 \dots a_k^{n_k} = 0$

con gli a_i nilpotenti. Ma allora posto $N = \max\{n_i\}$, A è N nilpotente

(ii) $\mathbb{Z}/2^N$. Se $a \in \mathbb{Z}/2^N$ e compare 2 nella fatt., allora $a = 2b \Rightarrow$
$$a^N = 2^N b^N = 0$$

se 2 non compare nella fatt. allora $(a, 2^N) = 1$ e a è invertibile

$$\bigoplus_{i \in \mathbb{N}} \mathbb{Z}/2^i \subseteq \prod_{i \in \mathbb{N}} \mathbb{Z}/2^i$$

gli el. hanno solo un numero di comp. $\neq 0$

Op. componente per componente

Suppongo sia N nilpotente allora prendo $(\underbrace{0 \_\_ 0}_{N}, 2, 0 \_\_ 0)$

e lui è $N+1$ nilpotente.

(3) $A = \mathrm{Mat}_N(\mathbb{k})$ $a, b \in A$ $k_1, \_\_, k_{N+1} \in \mathbb{k}$ distinti tali che

$a + k_i b$ è nilpotente $\forall i$.

Mostrare che a e b sono nilpotenti

Considero la matrice $\underset{\shortparallel}{a + xb}^{\,m(x)}$, con x variabile su $\mathbb{k}$.

$p_{m(x)}(t) = \det(a + xb - t\,id)$ ha grado n in x e grado n in t

c'è proprio un termine $a x^n$ e uno t^n (Pensarci un attimo)

$$t^n + \underbrace{x^n p_{n-1}(t) + x^{n-1} p_{n-2}(t) + \dots + x\,p_1(t) + p_0(t)}_{q(t,x)} \in \mathbb{k}[x,t]$$

$q(t,x) \in \underbrace{\mathbb{k}[t]}_{A}[x]$ e ha grado n in x

Si annulla per $n+1$ valori di $\mathbb{k}$ e il polinomio è a coeff in Dominio ($\mathbb{k}[t]$), allora

è il polinomio **NULLO** $\Rightarrow \forall x \quad \det(a + xb - t\,id) = t^n$

in particolare per $x = 0 \Rightarrow a$ è nilpotente

$a + xb \rightsquigarrow \frac{1}{x} a + b$ con $x \neq 0$ posso ripetere lo stesso ragionamento

$\frac{1}{x} a + b = y a + b$ e poi pongo $y = 0$

(4) A N-nilp. $a, b \in A$ $k_1 \_\_ k_{N+1} \in A$ e suppongo $a + k_i b$ Nilp. $\forall i$

È necessariamente vero che a, b nilpotenti?

NO $\mathbb{Z}/_{2^6}$ $(1 + 3k)$ $\forall k$ dispari $(1+3k)$ è nilpotente e ci

sono più di 7 dispari in $\mathbb{Z}/_{2^6}$ $\Rightarrow$ Non è necessariamente vero