

Esercizio 3

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

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

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

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

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

Elevo al quadrato

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

$\alpha^2, \beta^2 \in \mathbb{Q}$ 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.

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

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

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

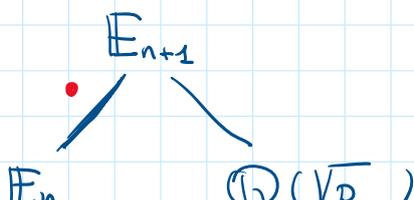
Claim: Grado $= 2^n$ Gal $(\mathbb{E}_n/\mathbb{Q}) = (\mathbb{Z}/2)^n$

Per induzione su n .

$n=1$ funzione $\mathbb{Q}(\sqrt{p_1}) \supseteq \mathbb{Q}$ $x^2 - p_1$ irr. grado 2 $\Rightarrow \mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$

Galois e tutto bello insomma

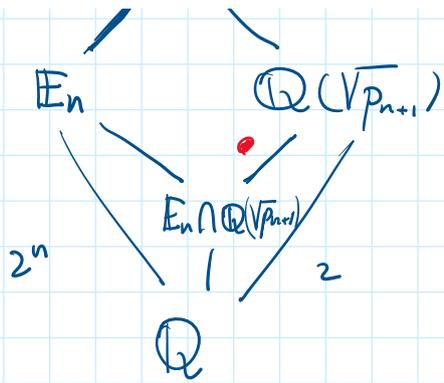
$n \Rightarrow n+1$



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

Per farlo è sufficiente dire che $[\mathbb{E}_{n+1} : \mathbb{E}_n]$ ha

grado 2 e questa ha grado 2 se l'estensione



grado 2 e questa ha grado 2 se l'estensione

$$\mathbb{Q}(\sqrt{p_{n+1}}) / \mathbb{Q}(\sqrt{p_{n+1}}) \cap E_n$$

ha grado 2. Per dimostrarlo mi basta dire che

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

Dimostrando:

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

$$\mathbb{Q}(\sqrt{p_{n+1}}) \begin{matrix} \nearrow \\ \searrow \end{matrix} \mathbb{Q}$$

Voglio escluderlo

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

Ma le sottost. di E_n le conosco tutte:

Per ip. induttiva $\text{Gal}(E_n/\mathbb{Q}) \cong (\mathbb{Z}/2)^n$. Le sottost. di grado 2 sono quindi

in biiezione con i sottogz. 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 $\sqrt{p_i}$

$$\sqrt{p_2} \quad \dots \quad \sqrt{p_n}$$

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

$\sqrt{p_1}$	$\sqrt{p_2}$	$\sqrt{p_3}$	$n=3$ $7 = 2^3 - 1$
$\sqrt{p_1 p_2}$	$\sqrt{p_1 p_3}$	$\sqrt{p_2 p_3}$	
$\sqrt{p_1 p_2 p_3}$			

Se adesso confronto $\mathbb{Q}(\sqrt{p_{n+1}})$

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

$$\mathbb{Z} \begin{matrix} \nearrow \\ \searrow \end{matrix} E_{n+1}$$

Per teorema foloires vale che

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

$$E_n \begin{matrix} \nearrow \\ \searrow \end{matrix} \mathbb{Q}(\sqrt{p_{n+1}}) \\ (\mathbb{Z}/2)^n \begin{matrix} \nearrow \\ \searrow \end{matrix} \mathbb{Z}$$

$(\mathbb{Z}/2)^n$ \mathbb{Q} $\mathbb{Z}/2$ $\mathbb{Q}(\sqrt[3]{2})$ $\mathbb{Q}(\sqrt[3]{2}) = (\mathbb{Z}/2) \times \mathbb{Z}/2 = (\mathbb{Z}/2)$

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

$\Leftarrow \frac{\gamma}{\delta} \in \mathbb{Q} \Rightarrow \frac{\gamma}{\delta} = q \quad \gamma = q\delta \quad \text{ten}$

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

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

$\Rightarrow \mathbb{Q}(\gamma) = \mathbb{Q}(\delta) \quad \exists a, b, c \in \mathbb{Q} \begin{matrix} \text{ } \\ \text{ } \\ \text{ } \end{matrix} \begin{matrix} \text{ } \\ \text{ } \\ \text{ } \end{matrix}$

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

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

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

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 enologica
- se 2 dei 3 uguali a 0 così:
 - $b, c = 0 \Rightarrow \delta = a \in \mathbb{Q} \quad \checkmark$
 - $a, c = 0 \Rightarrow \frac{\delta}{\gamma} \in \mathbb{Q} \quad \checkmark$
 - $a, b = 0 \Rightarrow \frac{\delta}{\gamma^2} \in \mathbb{Q} \quad \checkmark$

(iv) $p_1 \dots p_n$ in \mathbb{Z} primi distinti: $L_n = \mathbb{Q}(\sqrt[3]{p_1}, \dots, \sqrt[3]{p_n}, S_3)$

$[L_n : \mathbb{Q}]$ e $\text{Gal}(L_n/\mathbb{Q})$

Claim: $3^n \cdot 2$ grado

$\sqrt[3]{p_i} \xrightarrow{\text{id}} \sqrt[3]{p_i} \quad S_3 \rightarrow S_3^{-1}$

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

Per induzione su n : grado = $3^n \cdot 2$ $\text{Gal}(\mathbb{L}_n/\mathbb{Q}) = (\mathbb{Z}/3\mathbb{Z})^n \rtimes \mathbb{Z}/2\mathbb{Z}$, $\varphi: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z})^n$
 $1 \mapsto \begin{pmatrix} 2 & & \\ & \ddots & \\ & & 2 \end{pmatrix}$

$\sqrt[3]{2}$ $\sqrt[3]{3}$ S_3

$$\sigma_1: \begin{matrix} \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ \sqrt[3]{3} \rightarrow \sqrt[3]{3} \\ S_2 \rightarrow S_3 \end{matrix}$$

$$\sigma_2: \begin{matrix} \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ \sqrt[3]{3} \rightarrow \sqrt[3]{3} \\ S_3 \rightarrow S_3 \end{matrix}$$

$$\delta: \begin{matrix} \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ \sqrt[3]{3} \rightarrow \sqrt[3]{3} \\ S_3 \rightarrow S_3^{-1} \end{matrix}$$

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

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

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

$\langle \delta \rangle$ 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 S_3 e gli altri no.

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

Se so de $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, S_3) : \mathbb{Q}] = 3^2 \cdot 2$ ho finito

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

$$\begin{matrix} \sigma_1 & \longmapsto & (1, 0, 0) \\ \sigma_2 & \longmapsto & (0, 1, 0) \\ \delta & \longmapsto & (0, 0, 1) \end{matrix}$$

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

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

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

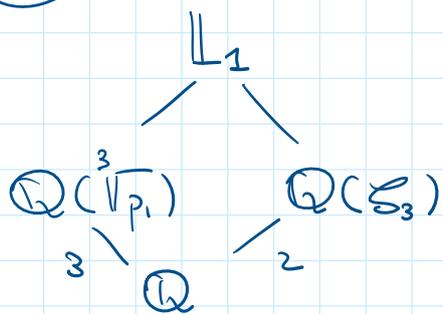
$$(0, 0, 1) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} (0, 0, 1) = (0, 0, 1) (1, 0, 1) = (0, 0) + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1+1 = (2, 0, 0)$$

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

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

Claim: grado $3^n \cdot 2$ $\text{Gal}(\mathbb{L}_n/\mathbb{Q}) = (\mathbb{Z}/3\mathbb{Z})^n \rtimes \mathbb{Z}/2\mathbb{Z}$

$n=1$



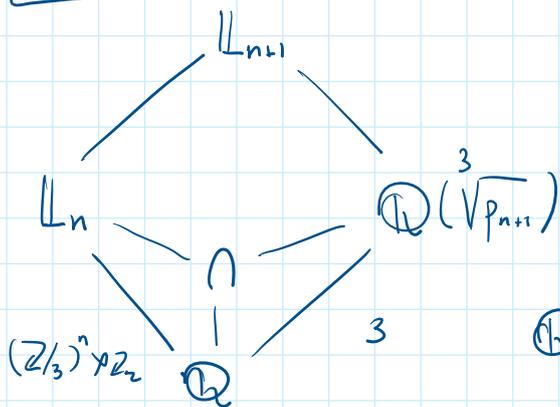
$$\sigma_2: \begin{matrix} \sqrt[3]{p_1} \rightarrow \sqrt[3]{p_1} \sigma_2 \\ S_3 \rightarrow S_3 \end{matrix} \quad \delta: \begin{matrix} _ \\ _ \end{matrix}$$

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

$$\varphi: \mathbb{Z}/2 \rightarrow \text{Aut}(\mathbb{Z}/3)$$

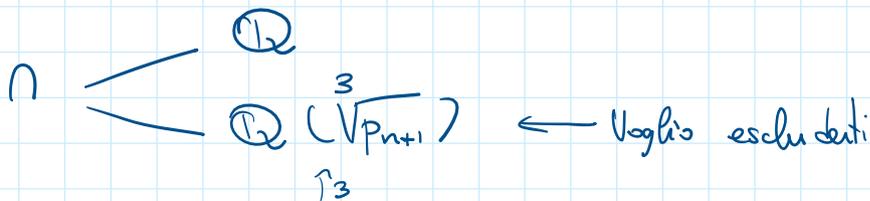
$$1 \mapsto (2)$$

$n \rightarrow n+1$



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

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



Stare cercando le sottoestensioni di grado 3 su \mathbb{Q} di L_n che corrispondono ai sottogruppi di indice 3 in $(\mathbb{Z}/3)^n \times \mathbb{Z}/2$

Sottoest. di grado 3:

$$\boxed{\sqrt[3]{p_1} \dots \sqrt[3]{p_n}}$$

$$\begin{matrix} \sqrt[3]{p_1} (S_3) & \dots & \sqrt[3]{p_n} (S_3) \\ \sqrt[3]{p_1} (S_3^2) & \dots & \sqrt[3]{p_n} (S_3^2) \end{matrix}$$

$$\sqrt[3]{p_1} \quad 0 \quad 1 \quad 2$$

Ho 3 scelte $\forall p_i$

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

1, 1, 2

$$2 \quad 2 \quad 1$$

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

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

$$(\mathbb{Z}/3)^n \rtimes_{\varphi} \mathbb{Z}/2 = G_n$$

Oss 1: gli elementi di G_n sono tutti di ordine 3 o 2

$$\left(\underbrace{1, 0, 1, 0, 1, 1, 1, 1}, \textcircled{1} \right) \left(\underbrace{1, 0, 1, 0, 1, 1, 1, 1}, 1 \right) = \left(\quad 0 \quad , 0 \right)$$

Oss 2: 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 $(\mathbb{Z}/3)^n$

$$a_1 x_1 + \dots + a_n x_n = 0$$

$$a_i \in \mathbb{Z}/3$$

$$x_1 + 2x_2 = 0$$

$$2x_1 + x_2 = 0$$

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

Oss 3: Dato che ogni $(\mathbb{Z}/3)^{n-1}$ è "uguale" agli altri e vero di Automorfismi, posso supporre che il mio iperpiano sia quello ident. delle prime $n-1$ coordinate

$$(\mathbb{Z}/3 \times \dots \times \mathbb{Z}/3 \times \mathbb{Z}_2) \rtimes \mathbb{Z}/2$$

$$(\underbrace{\mathbb{Z}/3 \times \dots \times \mathbb{Z}/3}_{n-1}) \times 0$$

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

$$\begin{array}{l} \left(0 \quad \quad \quad 0, \textcircled{0}, \underline{1} \right) \leftarrow \begin{array}{c} \textcircled{1} \\ \textcircled{2} \end{array} \\ \left(0 \quad \quad \quad 0, \textcircled{1}, \underline{1} \right) \leftarrow \\ \left(0 \quad \quad \quad 0, \textcircled{2}, \underline{1} \right) \leftarrow \end{array}$$

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

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

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

Definisco \mathcal{G} come nell'esempio e ci sono

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

(i) A anello finito $\Rightarrow N$ -t 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 nelle fatt., allora $a = 2b \Rightarrow a^N = 2^N b^N = 0$

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

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

1, 1, 1, 1, ...

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

Op. componente per componente

Suppongo sia N nilpotente allora prendo $(\underbrace{0, \dots, 0}_{N}, 2, 0, \dots, 0)$
 e lui è $N+1$ nilpotente.

(3) $A \cong \text{Mat}_N(\mathbb{K})$ $a, b \in A$ $k_1, \dots, k_{N+1} \in \mathbb{K}$ distinti tali che

$a+kb$ è nilpotente \forall .

Mostrare che a e b sono nilpotenti

Considero la matrice $a+xb$ con x variabile su k .

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

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

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

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

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

è il polinomio NULLO. $\Rightarrow \forall x \det(a+xb - tid) = t^n$

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 e poi pongo $y=0$

(4) A N-nilp. $a, b \in A$ $k_1 \dots k_{n+1} \in A$ e supponi $a+k_1b$ Nilp. $\forall i$

È necessariamente vero che a, b nilpotenti?

NO $\mathbb{Z}/26$ $(1+3k)$ $\forall k$ dispari $(1+3k)$ è nilpotente e ci sono più di 7 dispari in $\mathbb{Z}/26 \Rightarrow$ Non è necessariamente vero