Seminario

Andoni Latorre Galarraga

1.
Veamos que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es cíclico de orden $p-1$. Sea $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

$$\zeta^p - 1 = 0 \Rightarrow \sigma(\zeta)^p - 1 = 0$$

Tenemos que $\sigma(\zeta)$ es raiz p-ésima de la unidad. Ahora, por ser ζ raiz primitiva.

$$\sigma(\zeta) = \zeta^d$$

para $d \in \{1, \cdots, p-1\}$. Veamos que σ es automorfismo. Teniendo en cuenta que $\{\zeta, \zeta^2, \cdots, \zeta^{p-1}\}$ es base de $\mathbb{Q}(\zeta)/\mathbb{Q}$:

$$\begin{array}{rlcl} \sigma: & \mathbb{Q}(\zeta) & \longrightarrow & \mathbb{Q}(\zeta) \\ & q \in \mathbb{Q} & \longmapsto & q \\ & \zeta & \longmapsto & \zeta^d \\ & \zeta^2 & \longmapsto & \zeta^{2d} \\ & & \vdots & \\ & \zeta^{p-1} & \longmapsto & \zeta^{(p-1)d} \end{array}$$

Supongamos que $\sigma(\zeta^{k_1}) = \sigma(\zeta^{k_2})$ con $k_1 > k_2$.

$$\zeta^{dk_1} = \zeta^{dk_1} \Rightarrow 1 = \zeta^{d(k_1-k_2)} \Rightarrow p \mid d(k_1 - k_2)$$

pero p es primo y $d, (k_1 - k_2) \in \{1, \cdots, p-1\}$, que es contradictorio. Por lo tanto σ es inyectivo y

$$\sigma(\{\zeta, \zeta^2, \cdots, \zeta^{p-1}\}) = \{\zeta, \zeta^2, \cdots, \zeta^{p-1}\}$$

es decir, σ es automorfismo. Si llamamos σ_d al automorfismo que satisface $\zeta \longmapsto \zeta^d$. tenemos que

$$\begin{array}{rrcl} \varphi: & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) & \longrightarrow & ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \\ & \sigma_k & \longmapsto & \overline{k} \end{array}$$

Es isomorfismo de grupos

$$\sigma_a \circ \sigma_b : \zeta \longmapsto \zeta^{ab} \Rightarrow \varphi(\sigma_a \circ \sigma_b) = \overline{ab}$$

$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$, Probando que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es cíclico. Ahora,

$$|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) : \mathrm{Gal}(\mathbb{Q}(\zeta)/E)||\mathrm{Gal}(\mathbb{Q}(\zeta)/E)| =$$
$$= |\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$$
$$\Rightarrow [E : \mathbb{Q}]|\mathrm{Gal}(\mathbb{Q}(\zeta)/E)| = |\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$$
$$\Rightarrow 2|\mathrm{Gal}(\mathbb{Q}(\zeta)/E)| = |\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$$
$$\Rightarrow |\mathrm{Gal}(\mathbb{Q}(\zeta)/E)| = \frac{p-1}{2}$$

Como $\frac{p-1}{2}$ es divisor de $p-1$ existe un único subgrupo de orden $\frac{p-1}{2}$ (2.30 en el libro de rojo). Resumiendo, si $[E : \mathbb{Q}] = 2$ entonces solo existe un posible $\mathrm{Gal}(\mathbb{Q}(\zeta)/E)$ y por lo tanto $\exists! E$ por la correspondencia de Galois ya que $\mathbb{Q}(\zeta)/\mathbb{Q}$ es de Galois $p - 1 = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.
Supongamos que $E \subseteq \mathbb{R} \cap \mathbb{Q}(\zeta)$. Tenemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta) \cap \mathbb{R}] = 2$ ya que $\mathbb{Q}(\zeta) = (\mathbb{Q}(\zeta) \cap \mathbb{R})(i)$. Entonces,

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \big| \; 2 \\ \mathbb{Q}(\zeta) \cap \mathbb{R} \\ \big| \\ E \\ \big| \; 2 \\ \mathbb{Q} \end{array}$$

$\Rightarrow 4 \mid [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1 \Rightarrow p \equiv 1 (\mathrm{mod}\ 4)$
2.
i)
Las raices de $(x^3-3)(x^2-3)$ son $\{\sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2, \pm\sqrt{3}\}$.

$$\zeta_3 = e^{i\frac{2\pi}{3}} = \cos(\frac{2\pi}{3}) + i\sin(\frac{3\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$\zeta_3^2 = e^{i\frac{4\pi}{3}} = \cos(\frac{2\pi}{3}) + i\sin(\frac{4\pi}{3}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Veamos que

$$\left\{-\frac{\sqrt[3]{3}}{2} \pm i\frac{\sqrt[6]{3}}{2}, \pm\sqrt{3}\right\} \subset \mathbb{Q}(\sqrt[6]{3}, i)$$

Es suficiente con observar que $\sqrt[6]{3}^2 = \sqrt[3]{3}$ y $\sqrt[6]{3}^3 = \sqrt[2]{3}$. Veamos ahora que

$$\{\sqrt[6]{3}, i\} \subset \mathbb{Q}\left(-\frac{\sqrt[3]{3}}{2} \pm i\frac{\sqrt[6]{3}}{2}, \pm\sqrt{3}\right)$$

$$-\left(-\frac{\sqrt[3]{3}}{2} + i\frac{\sqrt[6]{3}}{2} - \frac{\sqrt[3]{3}}{2} - i\frac{\sqrt[6]{3}}{2}\right) = \sqrt[3]{3}$$

$$\frac{\sqrt{3}}{\sqrt[3]{3}} = \sqrt[6]{3}$$

$$\left(-\frac{\sqrt[3]{3}}{2} + i\frac{\sqrt[6]{3}}{2}\right) - \left(-\frac{\sqrt[3]{3}}{2} - i\frac{\sqrt[6]{3}}{2}\right) = i\sqrt[6]{3}$$

$$i\frac{\sqrt[6]{3}}{\sqrt[6]{3}} = i$$

Tenemos que $\mathbb{Q}(\sqrt[6]{3}, i) = \mathbb{Q}\left(-\frac{\sqrt[3]{3}}{2} \pm i\frac{\sqrt[6]{3}}{2}, \pm\sqrt{3}\right)$. $\mathbb{Q}(\sqrt[6]{3}, i)$ es el cuerpo de escisión de $(x^3-3)(x^2-3)$ sobre $\mathbb{Q}$ y $F/\mathbb{Q}$ es de Galois.
Las raices de $x^3 + \sqrt{3}$ son $-\sqrt[6]{3}$ y $\frac{\sqrt[6]{3}}{2} \pm i\frac{\sqrt[3]{3}^2}{2}$. Por un lado,

$$\left(\frac{\sqrt[6]{3}}{2} + i\frac{\sqrt[3]{3}^2}{2}\right) - \left(\frac{\sqrt[6]{3}}{2} - i\frac{\sqrt[3]{3}^2}{2}\right) = i\sqrt[3]{3}^2$$

$$i\frac{\sqrt[3]{3}^2}{\sqrt[6]{3}^4} = i$$

$$\Rightarrow F \subset \mathbb{Q}\left(-\sqrt[6]{3}, \frac{\sqrt[6]{3}}{2} \pm i\frac{\sqrt[3]{3}^2}{2}\right)$$

Por otro lado,

$$\sqrt[6]{3}^2 = \sqrt[3]{3} \Rightarrow \mathbb{Q}\left(-\sqrt[6]{3}, \frac{\sqrt[6]{3}}{2} \pm i\frac{\sqrt[3]{3}^2}{2}\right) \subset F$$

es decir, F es el cuerpo de escisión de $x^3 + \sqrt{3}$ sobre $\mathbb{Q}(\sqrt{3})$.

ii)

Consideramos

$$\sigma : \left\{ \begin{array}{ccc} \zeta & \longmapsto & \zeta^d \\ \sqrt[6]{3} & \longmapsto & \sqrt[6]{3} \end{array} \right.$$

Si $d = 2$

$$\sigma(\zeta^3) = \zeta^6 = 1 = \sigma(1)$$

Si $d = 3$

$$\sigma(\zeta^2) = \zeta^6 = 1 = \sigma(1)$$

Si $d = 4$

$$\sigma(\zeta^4) = \zeta^1 2 = 1 = \sigma(1)$$

Ninguno es automorfismo por no ser inyectivo. Con $d = 5$

$$\sigma : \zeta \longmapsto \zeta^5 \longmapsto \zeta$$

$$\sigma : \zeta^2 \longmapsto \zeta^4 \longmapsto \zeta^2$$

$$\sigma : \zeta^3 \longmapsto \zeta^3$$

Es automorfismo de orden 2. Ahora, consideramos

$$\tau : \left\{ \begin{array}{ccc} \zeta & \longmapsto & \zeta \\ \sqrt[6]{3} & \longmapsto & \zeta\sqrt[6]{3} \end{array} \right.$$

$$\tau : \sqrt[6]{3} \longmapsto \zeta\sqrt[6]{3} \longmapsto \zeta^2\sqrt[6]{3} \longmapsto \cdots \longmapsto \zeta^5\sqrt[6]{3} \longmapsto \sqrt[6]{3}$$

Es automorfismo de orden 6. Además podemos mandar $\sqrt[6]{3}$ a cualquier raiz de $x^6 - 3$ haciendo $\tau(\tau(\cdots(\tau(\sqrt[6]{3}))))$. Por lo tanto

$$\mathrm{Gal}(F/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \sigma\tau, \sigma\tau^2, \sigma\tau^3, \sigma\tau^4, \sigma\tau^5\}$$

Que es isomorfo a D_{12}.

iii)

$$|\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/E)||\mathrm{Gal}(F/E)| = |\mathrm{Gal}(F/\mathbb{Q})|$$

Como $6 = [E : \mathbb{Q}] = |\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/E)|$ y $|\mathrm{Gal}(F/\mathbb{Q})| = 12$.

$$|\mathrm{Gal}(F/E)| = 2$$

Que nos deja como opciones para $\mathrm{Gal}(F/E)$

$$\langle\sigma\rangle, \langle\tau^3\rangle, \langle\sigma\tau\rangle, \langle\sigma\tau^2\rangle, \langle\sigma\tau^3\rangle, \langle\sigma\tau^4\rangle, \langle\sigma\tau^5\rangle$$

Y los subcuerpos intermedios serían

$$\mathrm{Fix}\langle\sigma\rangle, \mathrm{Fix}\langle\tau^3\rangle, \mathrm{Fix}\langle\sigma\tau\rangle, \mathrm{Fix}\langle\sigma\tau^2\rangle$$

$$\mathrm{Fix}\langle\sigma\tau^3\rangle, \mathrm{Fix}\langle\sigma\tau^4\rangle, \mathrm{Fix}\langle\sigma\tau^5\rangle$$

iv)

No, D_{12} no teine elementos de orden 4 y por lo tanto no tiene subgrupos cíclicos de orden 4.