Teoría de números: 17 octubre

Clase pasada: Grupo de Galois de $\Phi_p$

Hoy: Grupo de Galois de $\Phi_p$ (Continuación)

---

Consideremos $\sigma \in Gal(\mathbb{Q}(\zeta) \backslash \mathbb{Q})$

entonces
$$\sigma(\zeta_p)^{p-1} + \cdots + \sigma(\zeta_p) + 1$$
$$= \sigma(\zeta_p^{p-1} + \cdots + \zeta_p + 1) = 0$$

Por lo tanto $\sigma(\zeta_p)$ es raíz de $\Phi_p(x)$.

Así
$$Gal(\mathbb{Q}(\zeta_p) \backslash \mathbb{Q}) \longrightarrow S_n$$
$$\sigma \longmapsto \{\zeta, \dots, \zeta^{p-1}\} \longmapsto \{\zeta^{\sigma(1)}, \dots, \zeta^{\sigma(p-1)}\}$$

donde $\sigma(\zeta^k) = \zeta^{\bar{\sigma}(k)}$ y $\bar{\sigma}(k) \in \{1, \dots, p-1\}$

$$\bar{\sigma} : \{1, 2, \dots, p-1\} \longmapsto \{1, 2, \dots, p-1\}$$

es injectiva pues las raíces son todas distintas

<u>Prop:</u> $\quad Gal(\mathbb{Q}(\zeta) \backslash \mathbb{Q}) \longrightarrow S_n$

es un homomorfismo de grupos inyectivo.

<u>Demostración:</u> $*$ homomorfismo

$$\sigma_1 \circ \sigma_2 (\zeta^j) = \sigma_1 \left(\zeta^{\bar{\sigma}_2(j)}\right) = \zeta^{\bar{\sigma}_1 \circ \sigma_2 (j)}$$

* Es inyectiva pues $\sigma$ está determinado por su efecto en $\zeta_p$ y sabemos $\mathbb{Q}(\zeta_p) \xrightarrow{\sigma} \mathbb{Q}(\zeta_p)$.

<u>COROLARIO</u>: $\left|Gal(\mathbb{Q}(\zeta_p) \backslash \mathbb{Q})\right|$ divide a $n!$

OBSERVACIÓN: consideremos $T_k : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$ inducido por $\zeta \longmapsto \zeta^k$.

$\Rightarrow \{T_1, \dots, T_{p-1}\} \subseteq Gal(\mathbb{Q}(\zeta) \backslash \mathbb{Q})$.

Recíprocamente, $\varphi \in Gal(\mathbb{Q}(\zeta) \backslash \mathbb{Q})$

$$\varphi(\zeta) \in \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$$

pues $\varphi(\zeta)$ es de nuevo raíz de $\Phi_p$.

pero

$\varphi(\zeta)$ determina totalmente a $\varphi$.

$$\Rightarrow \varphi \in \{T_1, T_2, \ldots, T_{p-1}\}$$

$$\Rightarrow |Gal(\mathbb{Q}(\zeta) \backslash \mathbb{Q})| = p-1$$

//

**COROL**: $\boxed{Gal(\mathbb{Q}(\zeta_p) \backslash \mathbb{Q}) \cong \mathbb{Z}/_{p-1}}$

Ejemplo revelador: $G_1 = \{Id, T_4\} \triangleleft \mathrm{Gal}(\zeta_5 \backslash \mathbb{Q})$

$$\mathbb{Z}/2 \triangleleft \mathbb{Z}/4$$

más aún

$$T_4(\zeta_5) + T_4(\zeta_5)^{-1} = T_4(\overbrace{\zeta + \zeta^{-1}}^{\alpha})$$

$$T_4(\alpha) = \alpha \qquad = \zeta^4 + \zeta^{-4}$$

$$= \zeta^{-1} + \zeta = \alpha$$

Esto implica:

$$T_4 : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$$

&

$$\boxed{T_4|_{\mathbb{Q}(\alpha)} = Id.}$$

---

$$\mathrm{Gal}(\mathbb{Q}(\zeta)\backslash\mathbb{Q}) \left\{ \begin{array}{c} \left.\begin{array}{c} \mathbb{Q}(\zeta) \\ | \\ \mathbb{Q}(\alpha) \end{array}\right\} \mathrm{Gal} = \{Id, T_4\} \\ | \\ \mathbb{Q} \end{array}\right.$$