Teoría de Números: 24 octubre

Clase pasada: Correspondencia de Galois

Hoy: Correspondencia de Galois II

Dado un polinomio ciclotómico $\Phi_p(x)$ construimos un campo

$$\begin{array}{l} \mathbb{Q}(\zeta_p) \\ \Big| \qquad \rightsquigarrow \; Gal(\Phi_p) \cong \mathbb{Z}/_{p-1} \cong (\mathbb{Z}/p)^* \\ \mathbb{Q} \end{array}$$

Pregunta: dado $H < Gal(\Phi_p)$ subgrupo ¿Existe un subcampo $K \leq \mathbb{Q}(\zeta_p)$ tal que $Gal(\mathbb{Q}(\zeta_p) \setminus K) \cong H$?

<u>Definición</u>: $H < Gal(\Phi_p)$ subgrupo.

$$\mathbb{Q}(\zeta)^H = \{\alpha \in \mathbb{Q}(\zeta) \mid \tau(\alpha) = \alpha \quad \forall \tau \in H\}$$

$\mathbb{Q}(\zeta)^H$ le llamaremos "campo fijado por H".

Eg: $p=7$. $\quad Gal(\Phi_7) \cong (\mathbb{Z}/7)^* \cong \mathbb{Z}/6$

existen dos subgrupos: $G_1 \cong \mathbb{Z}/2$ & $G_2 \cong \mathbb{Z}/3$

$[Gal : G_1] = 3 \qquad [Gal : G_2] = 2$.

Por lo tanto existen dos subcampos:

$$\begin{array}{c} \mathbb{Q}(\zeta_7) \\ | \\ \mathbb{Q}(\zeta_7)^{G_1} \\ | \\ \mathbb{Q} \end{array} \qquad \& \qquad \begin{array}{c} \mathbb{Q}(\zeta_7) \\ | \\ \mathbb{Q}(\zeta_7)^{G_2} \\ | \\ \mathbb{Q} \end{array}$$

¿Qué extensión de campo es esta?

Es decir; $\mathbb{Q}(\gamma)^{G_2} \cong \mathbb{Q}[x]/p(x)$ con $p \in \mathbb{Q}[x]$ irreducible

¿Qué polinomio es $p(x)$?

Calculemos: Consideramos $\beta = \gamma + \gamma^2 + \gamma^4$

Notar $G_2 = \{T_1, T_2, T_4\}$

$\cong$ {Residuos cuadráticos de $\mathbb{Z}/7$}

Observamos que

$$T_2(\beta) = \gamma^2 + \gamma^4 + \gamma = \beta$$

$$T_4 = \gamma^4 + \gamma^2 + \gamma = \beta$$

$$\Rightarrow \quad \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\gamma)^{G_2}$$

pues $\mathbb{Q}(\beta) \cong \mathbb{Q}[x] \big/ x^2+x+2$ y tiene por base$/\mathbb{Q}$

$\boxed{\text{Espacio Vectorial}/\mathbb{Q} \text{ de dimension } 2.}$

$\mathbb{Q}(\beta) = \mathcal{L}\{1, \beta\}$

EJER: $\beta^2+\beta+2=0$. Para finalizar

Deseamos ver: $\mathbb{Q}(\beta) = \mathbb{Q}(\gamma)^{G_2}$

Sabemos $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\gamma)^{G_2}$

la inclusión opuesta se sigue de lo siguiente:

tomemos $\sigma = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_6\gamma^6 \in \mathbb{Q}(\gamma)^{G_2}$

$$\left.\begin{array}{l} \Rightarrow \ T_2(\sigma) = \sigma \\ \& \ \ T_4(\sigma) = \sigma \end{array}\right\} \Rightarrow \boxed{\begin{array}{l} a_1 = a_2 = a_4 \\ a_3 = a_5 = a_6 \end{array}}$$

$$\Rightarrow \quad \sigma = a_0 + a_1(\gamma + \gamma^2 + \gamma^4) + a_3(\gamma^3 + \gamma^5 + \gamma^6)$$
$$= a_0 + a_1\beta + a_3(\gamma^3 + \gamma^5 + \gamma^6)$$

pero $\zeta^3+\zeta^5+\zeta^6 = -1-(\zeta+\zeta^2+\zeta^4)$

$$= -1-\beta$$

$$\Rightarrow \quad \gamma = a_0 - a_3 + (a_1 - a_3)\beta$$

$$= A + B\beta \in \mathbb{Q}(\beta)$$

$\Rightarrow \quad \mathbb{Q}(\zeta)^{G_2} \subseteq \mathbb{Q}(\beta)$ como deseabamos

$$\Rightarrow \quad \boxed{\mathbb{Q}(\zeta)^{G_2} = \mathbb{Q}(\beta)}$$

$$\Rightarrow \quad \begin{array}{l} \mathbb{Q}(\zeta_7) \\ \quad | \\ \mathbb{Q}(\zeta)^{G_2} = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/x^2+x+2 \\ \quad | \\ \mathbb{Q} \end{array}$$

Esto contesta qué campo es $\mathbb{Q}(\zeta)^{G_2}$.