Teoría de números: 15 octubre

Clase pasada: polinomios ciclotómicos.

Hoy: Grupo de Galois de Φ_p.

$\mathbb{Q}[x]/\Phi_p(x)$ — Campo ciclotómico

$|$

$\mathbb{Q}$

NOTAR: $\Phi_p(x) = x^{p-1} + \cdots + x + 1$

$p \in \mathbb{Z}$ primo.

Notación: $\mathbb{Q}[x]/\Phi_p = \mathbb{Q}(\gamma)$ donde γ raíz de $\Phi_p(x)$.

<u>Proposición:</u> $\mathbb{Q}(\gamma)$ es un espacio vectorial sobre $\mathbb{Q}$ de dimensión finita.

Demostración: Escribir una base **EJER**

Definición: $\dim_{\mathbb{Q}} \mathbb{Q}(\gamma) = p-1$ le llamaremos (ocasionalmente) el grado de la extensión $\mathbb{Q}(\gamma) \setminus \mathbb{Q}$.

= Al polinomio $\Phi_p(x)$ le asociamos = un grupo.

$$\mathrm{Aut}\left(\begin{array}{c}\mathbb{Q}(\gamma)\\ |\\ \mathbb{Q}\end{array}\right) = \mathrm{Gal}(\mathbb{Q}(\gamma)\setminus\mathbb{Q})$$

grupo de Automorfismos de $\mathbb{Q}(\gamma)$ como $\mathbb{Q}$-álgebra.

Afirmación: $\mathrm{Gal}(\mathbb{Q}(\gamma)\setminus\mathbb{Q})$ es (en efecto) un grupo finito.

Eg: $\boxed{p=5}$ Los siguientes automorfismos de $\mathbb{Q}$-algebra saltan a la vista

$$\mathbb{Q}(\gamma_5) \xrightarrow{T} \mathbb{Q}(\gamma_5) = \{a+b\gamma+c\gamma^2+d\gamma^3 \mid a,b,c,d \in \mathbb{Q}\}$$

con respecto a esta base

$\boxed{T_2(\gamma) = \gamma^2}$

$$\left.\begin{aligned} T_2(\gamma^2) &= \gamma^4 = -(1+\gamma+\gamma^2+\gamma^3) \\ T_2(\gamma^3) &= (\gamma^2)^3 = \gamma \\ T_2(1) &= 1 \end{aligned}\right\} \quad T_2 = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Por lo tanto tenemos

$$T_1, T_2, T_3, T_4$$

elementos de $\mathrm{Gal}(\mathbb{Q}(\gamma_5)\setminus\mathbb{Q})$

¿Son todos?

OBSERVAR:

$$T_2^2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix} = T_4$$

$$T_3 = T_2^3 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$T_2^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Por lo tanto tenemos la sig. estructura

$$(\mathbb{Z}/5)^* = \{1, 2, 3, 4\} \underset{\text{subgp}}{\geq} \{1, 4\}$$

$$= \text{grupo} \cong \mathbb{Z}/4$$

Residuos cuadráticos (mod 5).