Álgebra Moderna III 12 diciembre

Clase pasada: Correspondencia de Galois & #'s radicales.

Hoy: Ley de reciprocidad cuadrática

$p \in \mathbb{Z}$ primo

ζ_p = p-raíz primitiva de la unidad

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash] \\
\mathbb{Q}(\tau) \arrow[d, dash, "\text{grado } 2"] \\
\mathbb{Q}
\end{tikzcd}$$

$$\tau^2 = p^* := (-1)^{\frac{(p-1)}{2}} p$$

$q \in \mathbb{Z}$ primo $q \neq p$

$$\sigma_q(\tau) = \pm \tau$$

OBSERVAR:

$$\sigma_q(\tau) = \tau$$

$$\text{ssi}$$

$$\sigma_q \in Gal(\zeta_p \backslash \tau)$$

$$\text{ssi}$$

$$\left(\frac{q}{p}\right) = 1$$

Entonces

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau.$$

Pasamos a los anillos de enteros

$$\begin{array}{ccccc}
\mathbb{Q} & \subseteq & \mathcal{O}_p \subseteq & \mathbb{Q}(\zeta_p) \\
| & & & | \\
(q) & \subseteq & \mathbb{Z} \subseteq & \mathbb{Q}
\end{array}$$

$Q \leq \mathcal{O}_q$ ideal primo que contiene $q \in \mathcal{O}_q$.

Entonces, observar que:

$$\sigma_q(\tau) \equiv \tau^q \pmod{Q}.$$

Por lo tanto

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau \equiv \tau^q \pmod{Q}$$

$$\Rightarrow \quad \left(\frac{q}{p}\right) \equiv \tau^{q-1} \pmod{Q}$$

$$\equiv p^{*\left(\frac{q-1}{2}\right)} \pmod{Q}$$

$$\equiv \left(\frac{p^*}{q}\right) \pmod{Q}$$

$$\Rightarrow \quad \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \quad \text{pues } 2 \notin Q. \quad \blacksquare$$