Teoría de números : 10 octubre

Clase pasada: $p = a^2 - ab + b^2 \iff \left(\frac{-3}{p}\right) = 1$

$\iff p \equiv 1 \pmod 3$

Hoy: dado $n \in \mathbb{Z}$ caracterizar los primos $\in \mathbb{Z}$ tal que $\left(\frac{-n}{p}\right) = 1$.

Teorema (Gauss) [Reciprocidad cuadrática]

$p, q \in \mathbb{Z}$ primos distintos $(\neq 2)$.

Entonces $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

& 2 suplementos.

Para demostrar el teorema de arriba analizaremos campos que contienen a los racionales $\mathbb{Q}$ y sus automorfismos de $\mathbb{Q}$-álgebra.

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

& Φ_p es irreducible sobre $\mathbb{Q}$.

* basta encontrar un primo $q \in \mathbb{Z}$ tal que Φ_p es irred $/\mathbb{Z}/q$.

---

* (Gauss) Φ_p es irred en $\mathbb{Q}$ sii es irred en $\mathbb{Z}$.
& aplicar Eisenstein en $\mathbb{Z}$.

Prop: $\mathbb{Q}(\zeta_p) := \mathbb{Q}[x]/\Phi_p(x)$ $\quad p \in \mathbb{Z}$ primo

es un campo que contiene a $\mathbb{Q}$.

Demostración: $\mathbb{Q}(\zeta_p)$ evidentemente contiene a $\mathbb{Q}$.

Por otro lado, dado Φ_p es irreducible sobre $\mathbb{Q}$, se sigue que $\mathbb{Q}(\zeta)$ es campo. ∎

Afirmación: $\mathbb{Q}(\zeta)$ tiene automorfismos de $\mathbb{Q}$-álgebra.

1) $\mathbb{Q}(\zeta) \xrightarrow[\cong]{f} \mathbb{Q}(\zeta)$ isomorfismo de campo

2) $f|_{\mathbb{Q}} = Id$