

Algebra Moderna III : 22 de agosto 2

Curso pasado: $K = \mathbb{Q}[\sqrt{a}]$

$a \in \mathbb{Z}$ libre de

$$d = \begin{cases} a & a \equiv 1 \pmod{4} \\ 4a & a \equiv 2, 3 \pmod{4} \end{cases}$$

$\mathcal{R} =$ anillo
enteros
algebraicos $\subseteq \mathbb{Q}[\sqrt{a}]$

$$= \mathbb{Z} + \mathbb{Z} \left(\frac{d + \sqrt{d}}{2} \right) \subseteq \mathbb{Q}[\sqrt{a}]$$

$$R_p \in \mathcal{R} \subseteq \mathbb{Q}[\sqrt{a}]$$

$$\begin{array}{ccc} | & \updownarrow & \updownarrow \\ \langle p \rangle \in & \mathbb{Z} \subseteq & \mathbb{Q} \end{array}$$

extensiones
de campos &
anillos

\uparrow primo

$$R \cdot p \cap \mathbb{Z} = \langle p \rangle$$

¿Es $R \cdot p$ un ideal primo de \mathcal{R} ?

$$R \cdot p = \begin{cases} p_1 \cdot p_2 & \left(\frac{d}{p}\right) = 1 & \text{Excl} \\ p & \left(\frac{d}{p}\right) = -1 & \text{Incl} \\ p^2 & p \mid d & \text{Ram} \end{cases}$$

Reciprocidad Cuadrática:

$$\chi_d: (\mathbb{Z}/d\mathbb{Z})^* \longrightarrow \{1, -1\}$$

homomorfismo
de gprs.

&

$$R. p \text{ escinde} \iff \chi_d(p) = 1$$

$$R. p \text{ inerte} \iff \chi_d(p) = -1$$

OBSERVACIÓN $\mathbb{Z}/2\mathbb{Z}$ actúa en

y deja fijo \mathbb{Q} :

$$\begin{aligned} \alpha + \beta\sqrt{a} &\longmapsto \alpha + \beta\sqrt{a} \\ \alpha + \beta\sqrt{a} &\longmapsto \alpha - \beta\sqrt{a} \end{aligned}$$

$$\begin{array}{c} \mathbb{Q}[\sqrt{a}] \\ | \\ \mathbb{Q} \end{array}$$

Más aún: cuando $p \equiv 1 \pmod{4}$

$$x^2 + 1 = (x+a)(x-a) \quad \text{donde } a^2 \equiv -1 \pmod{p}$$

y en este caso

$$(x-a) = A \in \mathbb{Z}[i] - \mathbb{Q}[\sqrt{a}] = \mathbb{Q}[x] / x^2 - a$$

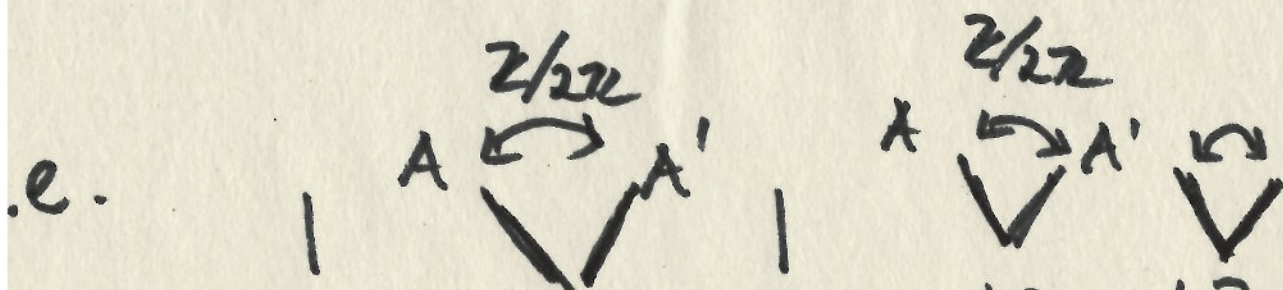
$$\begin{array}{c} | \quad | \quad | \\ \mathbb{Z} \in \mathbb{Z} \quad \text{---} \quad \mathbb{Q} \end{array}$$

$$A \cap \mathbb{Z} = \langle p \rangle$$

$$A' \cap \mathbb{Z} = \langle p \rangle$$

$$\mathbb{Z}[i] \cdot p = A \cdot A' \quad \text{e} \quad A' = (p, i+a)$$

$\mathbb{Z}/p\mathbb{Z}$ manda A en A' .



i.e. $\mathbb{Z}/2\mathbb{Z}$ i permuta las
raíces de $x^2 - a$
en $\mathbb{Q}[\sqrt{a}]$!

$\mathbb{Z}/2\mathbb{Z}$ es un gp asociado a

$x^2 - a$: Grupo de Galois
de $\mathbb{Q}[\sqrt{a}]/\mathbb{Q}$ o
del polinomio $x^2 - a$

¿ Para qué la historia de $\mathbb{Z}/2\mathbb{Z}$ y todo esto

- Demostraremos Reciprocidad
Cuadrática con estas técnicas

- Exhibir el gp de Galois de
un polinomio f i No es sólo