05/10 **Teoría de Galois**: $K/F$ ext^n de Galois

$\iff$ ·) separable ✓
·) normal

$\mathbb{Q}(\alpha) = K = \mathbb{Q}[x]/(f_{\mathbb{Q}}^{\alpha})$
$|$
$\mathbb{Q}$

$f = (x-\alpha_1)\dots(x-\alpha_n)$

$L$ = campo de descomposición de $f$.
$= \mathbb{Q}(\alpha_1, \dots, \alpha_n)$

$G = Gal(L/\mathbb{Q}) = Aut(L/\mathbb{Q})$. $|G| = [L:\mathbb{Q}]$

$G \curvearrowright \{\alpha_1, \dots, \alpha_n\}$ $G \hookrightarrow S_n$

Si $K = L \iff K/\mathbb{Q}$ es Galois.

En gral, $L$ es la cerradura de Galois de $K/\mathbb{Q}$.

**Ejemplo** $K = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ es Galois.

$\Phi_n$ es el pol. mínimo de $\zeta_n$ sobre $\mathbb{Q}$.

$\sigma_a : \mathbb{Q}(\zeta_n) \longrightarrow \mathbb{Q}(\zeta_n)$
$\zeta_n \longmapsto \zeta_n^a$, $mcd(a, n) = 1$

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$
$\sigma_a \longmapsto a \text{ mód } n$.

**Ejemplo** $K = \mathbb{Q}(\sqrt[3]{2})$.

$f = x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$

$L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. $Gal(L/\mathbb{Q}) \simeq S_3$.

$\sigma: \sqrt[3]{2} \longmapsto \zeta_3\sqrt[3]{2}$, $\zeta_3 \longmapsto \zeta_3$

$\tau: \zeta_3 \longmapsto \zeta_3^2$, $\sqrt[3]{2} \longmapsto \sqrt[3]{2}$

$ord(\sigma) = 3$ $ord(\tau) = 2$.

$\sigma\tau = \tau\sigma^2 \neq \tau\sigma$ $\langle\sigma, \tau\rangle = G \simeq S_3$.

**Proposición** Si $K/\mathbb{Q}$ es una ext^n de Galois, entonces $\forall$ encaje $\sigma: K \hookrightarrow \mathbb{C}$, tiene la misma imagen.

En particular, ·) o todos $\sigma$ son reales
$r_1 = [K:\mathbb{Q}]$
·) o todos $\sigma$ son complejos
$r_2 = \frac{1}{2}[K:\mathbb{Q}]$.

**Demostración** Una extn finita $K/F$ es normal $\iff$ todo encaje $\sigma : K \hookrightarrow \overline{F}$ tiene imagen $\sigma(K) = K$. $\square$

**Correspondencia de Galois**: Dada una extn. finita $K/\mathbb{Q}$, que es de Galois, consideremos $G = \mathrm{Gal}(K/\mathbb{Q})$.

A una subextn $F \subseteq K$ asociamos $H = \mathrm{Gal}(K/F) \subseteq G$.

Viceversa, a $H \leq G$, asociamos el subcampo fijo

$$F = K^H = \{ \alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H \}$$

$$\{\text{subcampos } F \subseteq K\} \underset{K^H \ \longleftarrow\!\shortmid\ H}{\overset{F \ \mapsto\ \mathrm{Gal}(K/F)}{\overset{\longrightarrow}{\underset{\longleftarrow}{1:1}}}} \{\text{subgrupos } H \leq G\}$$

1) $F \subseteq F' \Rightarrow H' \subseteq H$. $\qquad H \subseteq H' \Rightarrow K^{H'} \subseteq K^{H}$

2) $[K:F] = |H| \qquad [F:\mathbb{Q}] = [G:H]$

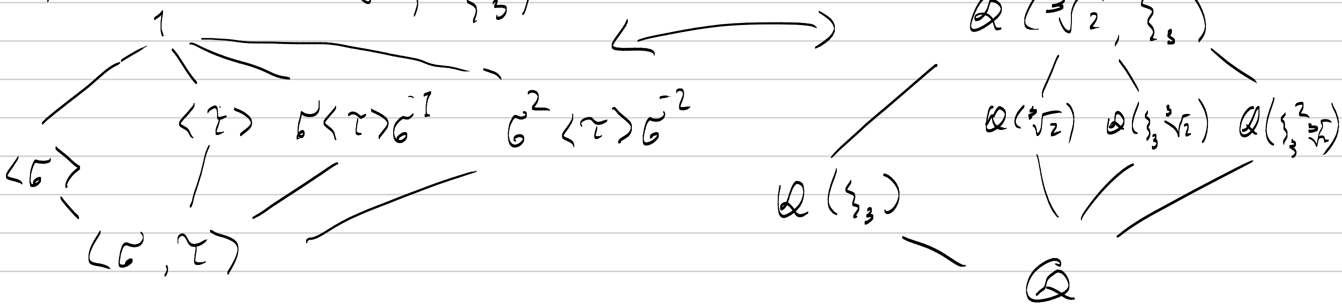
3) $F/\mathbb{Q}$ es normal $\iff$ $H \subseteq G$ es normal.

en este caso $\mathrm{Gal}(F/\mathbb{Q}) \simeq G/H$

4) $F \simeq F' \iff H$ y $H'$ son conjugados.

$\square$

**Ejemplo** $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$




**Problema inverso de Galois**: cualquier gpo finito $G$ es $\simeq \mathrm{Gal}(K/\mathbb{Q})$

**Ejemplo** $f = x^n - x - 1 \in \mathbb{Q}[x]$ es irreducible,

$K =$ campo de desc. de $f \Rightarrow \mathrm{Gal}(K/\mathbb{Q}) \simeq S_n$

Para $G$ abeliano.

**Proposición** Cualquier gpo abeliano finito puede ser realizado como el gpo de Galois de $K/\mathbb{Q}$.

**Demostración** $\forall\, p$ primo $\quad Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$

es cíclico de orden $p-1$

$G$ abeliano finito $\Rightarrow C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s} \simeq G$.

Teorema de Dirichlet: $\exists\ p_1, \dots, p_s$ diferentes primos

t.q. $p_i \equiv 1 \pmod{n_i}$ para $i = 1, \dots, s$.

$K = \mathbb{Q}(\zeta_{p_1 \cdots p_s})$

$G = Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/p_1 \cdots p_s)^\times \simeq (\mathbb{Z}/p_1\mathbb{Z})^\times \cdots (\mathbb{Z}/p_s\mathbb{Z})^\times$

$\forall i \quad \exists\, H_i < (\mathbb{Z}/p_i\mathbb{Z})^\times$ t.q. $(\mathbb{Z}/p_i\mathbb{Z})^\times / H_i \simeq C_{n_i}$

$G/(H_1 \times \cdots \times H_s) \simeq C_{n_1} \times \cdots \times C_{n_s}$. $\square$

**Ejemplo** $C_3 = ?$ $\qquad p = 7 \equiv 1 \pmod 3$

$$Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times$$

Hay subgrupo de índice 3

$$H = \langle \tau : \zeta_7 \mapsto \zeta_7^{-1} \rangle$$

$K^H = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ un subcampo cúbico con $Gal(K^H/\mathbb{Q}) \simeq C_3$.

$$\begin{tikzcd}[column sep=small] & 1 \arrow[dl, dash] \arrow[dr, dash] & \\ \{1,6\} \arrow[dr, dash] & & \{1,2,4\} \arrow[dl, dash] \\ & (\mathbb{Z}/7\mathbb{Z})^\times & \end{tikzcd} \quad \longleftrightarrow \quad \begin{tikzcd}[column sep=small] & \mathbb{Q}(\zeta_7) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{-7}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

**Teorema (Kronecker-Weber)**

Sea $K/\mathbb{Q}$ una extensión abeliana

($\Leftrightarrow Gal(K/\mathbb{Q})$ es abeliano)

entonces, $\exists\, n$ t.q. $K \subseteq \mathbb{Q}(\zeta_n)$.

**Demostración** Washington, "Cyclotomic fields", Ch. 14.

**Ejemplo** $K = \mathbb{Q}(\sqrt{d})$.

•) $p$ primo impar, $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$

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

·) $\sqrt{-1} \in \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ ·) $\sqrt{2} \in \mathbb{Q}(\zeta_8)$

(*) <u>Dirichlet</u>: $\forall n$ $\forall a$ tq. $\text{mcd}(a,n) = 1$

$\exists p$ primo t.q. $p \equiv a \pmod n$.

<u>Demostración</u>

$$\lim_{N\to\infty} \frac{\#\{p \text{ primo} \leq N \mid p \equiv a \pmod n\}}{\#\{p \text{ primo} \leq N\}} = \frac{1}{\varphi(n)}$$

## § Acción de $Gal(K/\mathbb{Q})$ sobre los ideales.

**Proposición** Sea $K/\mathbb{Q}$ extn de Galois, $\sigma: Gal(K/\mathbb{Q})$.

1) $\alpha \in \mathcal{O}_K \Rightarrow \sigma(\alpha) \in \mathcal{O}_K$.

2) $I \subseteq \mathcal{O}_K \Rightarrow \sigma(I) = \{\sigma(\alpha) \mid \alpha \in I\}$ es tb. un ideal.

Si $I = (\alpha_1, \dots, \alpha_n) \Rightarrow \sigma(I) = (\sigma(\alpha_1), \dots, \sigma(\alpha_n))$

3) $\mathcal{O}_K / I \simeq \mathcal{O}_K / \sigma(I)$.

4) $\mathfrak{p} \subset \mathcal{O}_K$ es primo $\Rightarrow \sigma(\mathfrak{p}) \subset \mathcal{O}_K$ es primo,

$\mathfrak{p} \mid p \Rightarrow \sigma(\mathfrak{p}) \mid p$, $f_\mathfrak{p} = f_{\sigma(\mathfrak{p})}$.

**Dem** 1) Si $\alpha$ es una raíz de $f \in \mathbb{Z}[x]$ mónico $\sigma(\alpha)$ es tb. una raíz de $f$.

2) fácil.

3)
$$\mathcal{O}_K \longrightarrow \mathcal{O}_K / \sigma(I) \rightsquigarrow \mathcal{O}_K / I \simeq \mathcal{O}_K / \sigma(I)$$
$$\alpha \longmapsto \sigma(\alpha) + \sigma(I)$$

4) $\mathfrak{p} \subset \mathcal{O}_K$ primo $\Leftrightarrow \mathcal{O}_K / \mathfrak{p}$ es dominio

$\mathcal{O}_K / \mathfrak{p} \simeq \mathcal{O}_K / \sigma(\mathfrak{p}) \Rightarrow \sigma(\mathfrak{p})$ primo.

$\Rightarrow \mathcal{O}_K / \mathfrak{p} \simeq \mathcal{O}_K / \sigma(\mathfrak{p}) \simeq \mathbb{F}_{p^f}$.

$\mathfrak{p} \mid p \Leftrightarrow p \in \mathfrak{p} \Rightarrow p = \sigma(p) \in \sigma(\mathfrak{p}) \Leftrightarrow \sigma(\mathfrak{p}) \mid p$.

$\square$

**Conclusión**: Si $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$

$G \curvearrowright \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$

**Ejemplo** $K = \mathbb{Q}(\sqrt{d})$ $\quad Gal(K/\mathbb{Q}) = \{1, \sigma\}$

$$\left(\frac{d}{p}\right) = +1 \Rightarrow \quad p\mathcal{O}_K = \mathfrak{p}\cdot\sigma(\mathfrak{p})$$

$$\sigma : \sqrt{d} \longmapsto -\sqrt{d}.$$

**Lema (Tate)** Sean $A$ un anillo conmutativo, $G$ gpo finito, $G \curvearrowright A$.

$$A^G = \{a \in A \mid \sigma(a) = a \quad \forall \sigma \in G\}$$

Sean $R$ un dominio, $\varphi, \psi$ homomorfismos

$$A^G \subset A \overset{\varphi}{\underset{\psi}{\rightrightarrows}} R \qquad \text{t.q.} \quad \varphi|_{A^G} = \psi|_{A^G}$$

entonces, $\varphi = \psi \circ \sigma$ para algún $\sigma \in G$.

**Teorema** Para una extn de Galois $K/\mathbb{Q}$, si $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_K$ son primos t.q. $\mathfrak{p}_1, \mathfrak{p}_2 \mid p$, entonces $\exists\ \sigma \in Gal(K/\mathbb{Q})$ t.q. $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$

**Dem** $\mathbb{Z} = \mathcal{O}_K^G \subset \mathcal{O}_K \overset{\varphi_1}{\underset{\varphi_2}{\rightrightarrows}} \overline{\mathbb{F}_p}$

$$\varphi_1|_{\mathbb{Z}} = \varphi_2|_{\mathbb{Z}}$$

$\mathfrak{p}_1 = \ker(\mathcal{O}_K \xrightarrow{\varphi_1} \overline{\mathbb{F}_p})$

$\mathfrak{p}_2 = \ker(\mathcal{O}_K \xrightarrow{\varphi_2} \overline{\mathbb{F}_p})$ $\quad$ Lema de Tate $\Rightarrow$

$$\exists\ \sigma \in G \quad \text{t.q.} \quad \varphi_1 = \varphi_2 \circ \sigma$$

$$\underset{\sigma(\mathfrak{p}_1)}{\underset{\|}{\sigma(\ker(\varphi_1))}} = \underset{\mathfrak{p}_2}{\underset{\|}{\ker(\varphi_2)}}$$

$\square$

**Proposición** Sea $K/\mathbb{Q}$ Galois, $p \in \mathbb{Z}$ primo racional

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Luego, $f_1 = \cdots = f_s$ y $e_1 = \cdots = e_s$.

**Dem** Si $\mathfrak{p}_i = \sigma(\mathfrak{p}_j) \Rightarrow f_i = f_j$.

La acción es transitiva $\Rightarrow f_1 = \cdots = f_s$

$$p\mathcal{O}_K = \sigma(p)\mathcal{O}_K = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_s)^{e_s}$$

$$= \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

$e(\mathfrak{p}_i) = e(\sigma(\mathfrak{p}_i))$ por la unicidad de desc. en ideales primos. $\square$

**Ejemplo** $K = \mathbb{Q}(\zeta_n)$ $\qquad n = \prod_p p^{v_p(n)}$

$e_p = \varphi(p^{v_p(n)})$ $\qquad f_p = $ orden de $p$ mód $\dfrac{n}{p^{v_p(n)}}$

**Notación** $K/\mathbb{Q}$ Galois, $p \in \mathbb{Z}$.

$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$

$$\left\{ \begin{array}{l} f_p = f_1 = \cdots = f_s \\ e_p = e_1 = \cdots = e_p. \\ g_p = s. \end{array} \right.$$

$\sum_i f_i e_i = [K : \mathbb{Q}]$.

$e_p f_p g_p = [K : \mathbb{Q}]$.

**Ejemplo** $K = \mathbb{Q}(\sqrt[3]{19})$, $\quad L = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$.

$F = \mathbb{Q}(\zeta_3)$

$$\begin{tikzcd} & L \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\ K \arrow[dr, dash, "3"'] & & F \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

**Nota**:

$$\begin{tikzcd} \mathfrak{q} \arrow[d, dash] & \subset & \mathcal{O}_L \arrow[d, dash] \arrow[r, two heads] & \mathcal{O}_L/\mathfrak{q} \arrow[d, dash] \\ \mathfrak{p} \arrow[d, dash] & \subset & \mathcal{O}_K \arrow[d, dash] \arrow[r, two heads] & \mathcal{O}_K/\mathfrak{p} \arrow[d, dash] \\ p & \in & \mathbb{Z} \arrow[r, two heads] & \mathbb{F}_p \end{tikzcd}$$

$f(\mathfrak{p}) \mid f(\mathfrak{q})$

$\Delta_F = -3$, $\quad \Delta_K = -3 \cdot 19^2$, $\quad \Delta_L = -3^3 \cdot 19^4$.

•) $p = 3$. $\qquad p\mathcal{O}_F = \mathfrak{r}^2$ $\qquad \underline{2 \mid e_3}$

$p\mathcal{O}_L = \mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2$ $\qquad f_1 = f_2 = f_3 = 1$.

$p\mathcal{O}_K = \mathfrak{p}^2 \cdot \mathfrak{p}'$. $\qquad f(\mathfrak{p}) = f(\mathfrak{p}') = 1$.

$e(\mathfrak{p}) = 2$.

$$\left. \underbrace{e_3}_{\substack{\text{divisible} \\ \text{por } 2}} \cdot f_3 \underbrace{g_3}_{\geq 2} = 6 \right\} \Rightarrow \begin{array}{l} e_3 = 2 \\ f_3 = 1 \\ g_3 = 3. \end{array}$$

•) Si $p \equiv 2 \ (3) \Rightarrow$ $\qquad p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, $\qquad f(\mathfrak{p}) = 1$

$2 \mid f_p \qquad g_p \geq 2$ $\qquad f(\mathfrak{p}') = 2$.

$$e_p \cdot \underbrace{f_p} \cdot \delta_p = 6 \Rightarrow e_p = 1, \quad f_p = 2, \quad \delta_p = 3.$$

$$p\mathcal{O}_L = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 \qquad f_1 = f_2 = f_3 = 2$$

·) $p \equiv 1 \ (3)$, $p$ no es cubo mód 19.

$p$ es inerte en $K$. $p\mathcal{O}_K$ primo, $f = 3$.

$$p\mathcal{O}_F = \mathfrak{q}\mathfrak{q}' \Rightarrow e_p \geq 2$$

$$e_p \underbrace{f_p}_{3|\cdot\cdot} \underbrace{\delta_p}_{\geq 2} = 6. \Rightarrow f_p = 3, \quad \delta_p = 2.$$

$$p\mathcal{O}_L = \mathfrak{q}_1 \mathfrak{q}_2 \qquad f_1 = f_2 = 3.$$