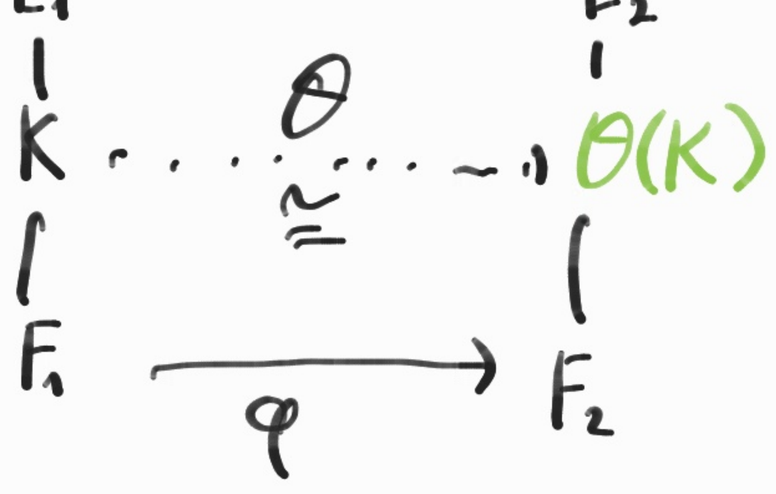
Teorema: Sea $\varphi: F_1 \to F_2$ un isomorfismo de campos y sean E_1 una cerradura algebr algebraica de F_1. Entonces φ se extiende a un isomorfismo de E_1 en E_2.

Dem:

Sea $\mathcal{P}$ el conjunto de todos los pares (K, θ) con $F_1 \subseteq K \subseteq E_1$ y θ es un morfismo de K en E_2 que extiende a φ



Ordenamos $\mathcal{P}$ como: $(K_2, \theta_2) \leq (K_1, \theta_1)$ si $K_2 \subseteq K_1$ y θ_2 es la restriccion de θ_1

Se tiene que $\mathcal{P} \neq \emptyset$, $(F_1, \varphi) \in \mathcal{P}$. No es dificil

ver que cada cadena en $\mathcal{P}$ tiene cota superior

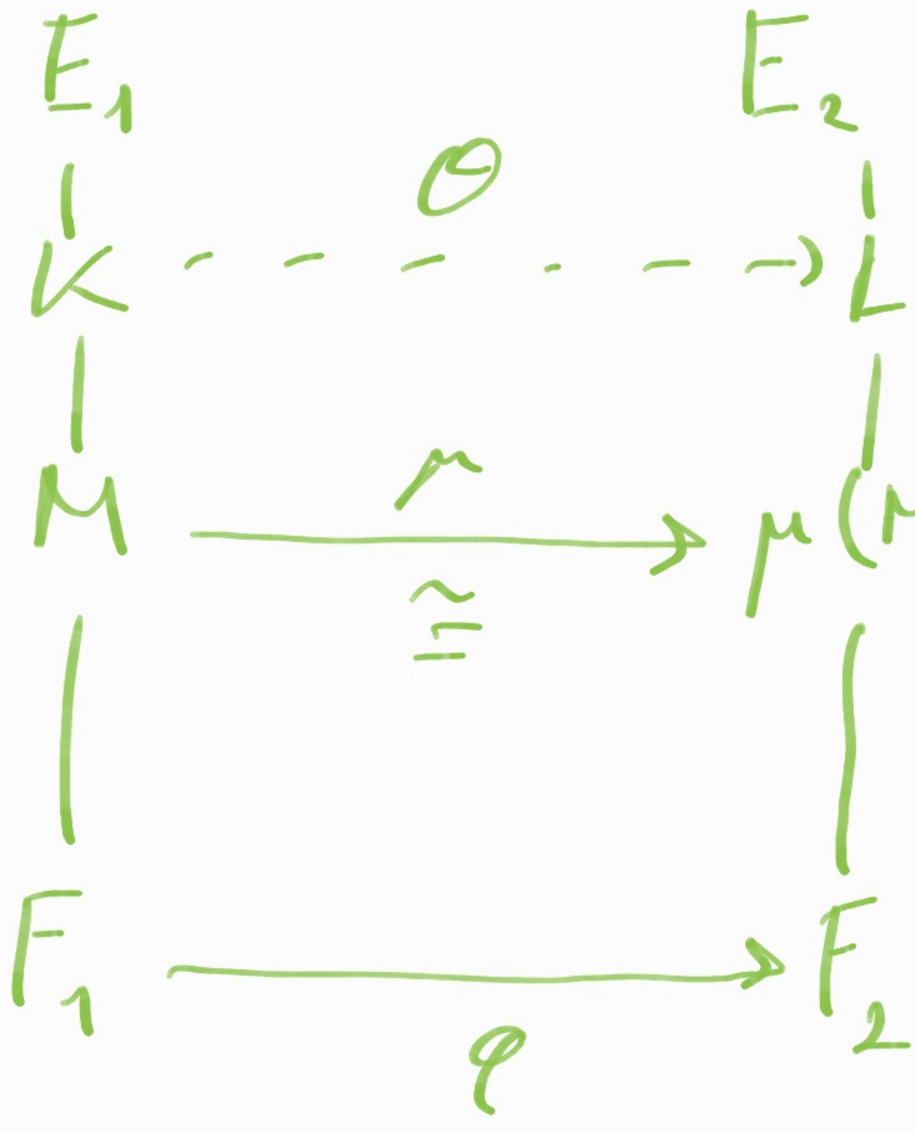
Por el Lema de Zorn $\mathcal{P}$ tiene maximos.. Sea

$(M, \mu) \in \mathcal{P}$ un máximo.

Afirmamos que M es una cerradera algebraica de F_1. Sea $0 \neq f_1 \in F_1[x]$. Como f_1 se escinde sobre E_1, por un lema anterior podemos tomar un campo de descomposicion K de f_1 tal que $M \subseteq K \subseteq E_1$. De la misma manera para el polinomio $\hat{\mu} f_1$ podemos tomar un campo de descomposicion L tal que $\mu(K) \subseteq L \subseteq E_2$

Por un teorema anterior μ se extiende a

un isomorfismo $\theta : K \to L$. Por lo tanto



$(K, \theta) \in \mathcal{P}$ y

Ademas

$(M, \mu) \leq (K, \theta)$

La maximalidad de M implica que $M = K$ y $\mu = \theta$

Por lo tanto el polinomio f_1 se escinde sobre M.

Esto quiere decir que M es una cerradura alg. de F_1. Entonces $\mu(M)$ es una cerradura alg. de F_2.

Ahora como $E_1 \supseteq F_1$ es una extension algebraica y $E_1 \supseteq M$ entonces $M = E_1$.

Analogamente $\mu(M) = E_2$. Por lo tanto μ extiende a ℓ a un isomorfismo

$$\mu : E_1 \to E_2.$$

Cor. Sea F cualquier campo y sean E_1 y E_2 cerraduras algebraicas de F. Entonces E_1 y E_2 son F-isomorfas.

Teoría de Galois

La idea de la teoria de Galois es asociar a cada extension de campos un grupo. Esto nos permite trasladar preguntas de campos a grupos donde tal vez sean más sencillas.

Por ejemplo, dado un polinomio $f \in \mathbb{Q}[x]$ ¿Cómo podemos resolver la ecuación $f(x)=0$ en $\mathbb{C}$ dando las soluciones explicitas?

Consideremos el polinomio $x^3-2 \in \mathbb{Q}[x]$. Sus raices son tres:

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\left(\frac{-1 \pm \sqrt{-3}}{2}\right)$$

Notemos que estas raices están expresadas solo usando operaciones aritmeticas basicas y radicales. ¿Cuándo podemos hacer esto para cualquier polinomio $f(x) \in \mathbb{Q}[x]$? Esta pregunta la podemos pensar tomando el campo de descomposicion E de un polinomio $f \in \mathbb{Q}[x]$. Entonces tenemos una extension $\mathbb{Q} \subseteq E$.

Galois probó que las raices de f no siempre se pueden expresar usando operaciones aritmeticas elementales y radicales.

Def: Sea $F \subseteq E$ una extensión de campos. Denotamos $Aut(E)$ el conjunto de todos los isomorfismos de E en E. Definimos el grupo de Galois de la extencion $F \subseteq E$ como $Gal(E/F) = \{\sigma \in Aut(E) / \sigma \text{ es un } F\text{-isomorfismo}\}$.

Consideremos la extension $\mathbb{R} \subseteq \mathbb{C}$.

$Gal(\mathbb{C}/\mathbb{R}) = \{e, \sigma\} \cong \mathbb{Z}_2$

Si σ es un $\mathbb{R}$-isomorfismo de $\mathbb{C}$ en $\mathbb{C}$, entonces

$-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2 \quad \therefore \sigma(i) = \begin{cases} i \\ -i \end{cases}$

Si $\sigma(i) = i$, entonces $\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i)$

$= a + bi \quad \therefore \sigma = \text{Identidad}$

Si $\sigma(i) = -i$, entonces σ es la conjugacion compleja

Def: Sea E un campo y H un subgrupo de $Aut(E)$. Definimos el campo fijo de H como $Fix(H) = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. $\subseteq F$

En general, $\mathrm{Fix}(\mathrm{Gal}(E/F)) \supseteq F$ y $\mathrm{Gal}(E/\mathrm{Fix}(H)) \supseteq H$ para $H \subseteq \mathrm{Aut}(E)$

$$\mathrm{Fix}(\mathrm{Gal}(\mathbb{C}/\mathbb{R})) = \{\alpha \in \mathbb{C} \mid e(\alpha)=\alpha \text{ y } \overline{(\alpha)}=\alpha\} = \mathbb{R}$$

Para el polinomio $x^3-2 \in \mathbb{Q}[x]$ podemos considerar la extensión $E=\mathbb{Q}[\sqrt[3]{2}] \supseteq \mathbb{Q}$ $\min_{\mathbb{Q}}(\sqrt[3]{2}) = x^3-2$.

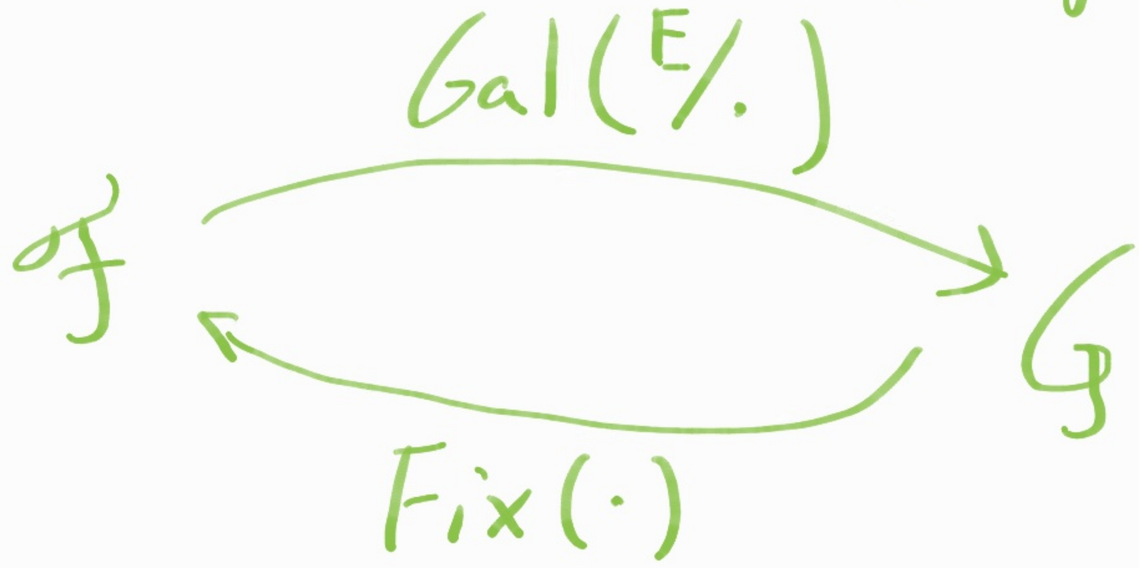
$\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, $\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$.

$\Rightarrow \sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Por lo tanto $\sigma = e$. $\mathrm{Gal}(E/F) = \{e\}$

y así $\mathrm{Fix}(\mathrm{Gal}(E/F)) = E \supsetneq \mathbb{Q}$

Sea $F \subseteq E$ una extension y $G = Gal(E/F)$.

Sea $\mathcal{F} = \{K \mid F \subseteq K \subseteq E\}$ y $\mathcal{G} = \{H \mid H \leq G\}$



Lema: Definimos $f: \mathcal{G} \to \mathcal{F}$ y $g: \mathcal{F} \to \mathcal{G}$ como $f = Fix(\cdot)$ y $g = Gal(E/\cdot)$. Entonces:

a) $g(f(H)) \geq H$ y $f(g(K)) \geq K$ para $H \in \mathcal{G}$ y $K \in \mathcal{F}$.

b) Si $H_1 \subseteq H_2$, ent $f(H_1) \geq f(H_2)$ para $H_i \in \mathcal{G}$

c) Si $K_1 \subseteq K_2$, ent $g(K_1) \geq g(K_2)$ para $K_i \in \mathcal{F}$.