Teorema fundamental de la teoria de Galois

Sea $E \geq F$ una extensión de Galois con $G = Gal(E/F)$. Escribimos:

$\mathcal{F} = \{K / F \subseteq K \subseteq E\}$ y $\mathcal{G} = \{H / H \leq G\}$.

i) Las asignaciones $f = Fix(\cdot)$ y $g = Gal(E/\cdot)$ son biyecciones entre $\mathcal{F}$ y $\mathcal{G}$ que son inversa una de la otra e invierten el orden.

ii) Si $g(K) = H$, entonces $[E : K] = |H|$ y $[K : F] = [G : H]$. En particular, $[E : F] = |G|$.

iii) Si $g(K) = H$ y $\sigma \in G$, entonces $g(\sigma(K)) = H^{\sigma}$, el conjugado de H por σ en G. También, $H \trianglelefteq G$ si y solo si $K \geq F$ es de Galois y en este caso $Gal(K/F) \cong G/H$.

Dem:

i) Ya sabemos que f, g son biyecciones entre los

$\mathcal{F}_0 \subseteq \mathcal{F}$ y $\mathcal{G}_0 \subseteq \mathcal{G}$ inversas una de la otra que invierten el orden. Como la extensión $E \supseteq F$ es finita, $\mathcal{G}_0 = \mathcal{G}$. Además como $F \subseteq E$ es de Galois tenemos que $\mathcal{F}_0 = \mathcal{F}$

ii) Sea $g(K) = H$ con $K \in \mathcal{F}$ y $H \in \mathcal{G}$. Como $K \subseteq E$ es Galois, $|H| = |Gal(E/K)| = [E:K]$ en particular, $|G| = [E:F]$. Como $K \in \mathcal{F}$, se tiene que $[E:F] = [E:K][K:F]$. Así que $|G| = |H|[K:F]$. Por lo tanto. $[G:H] = [K:F]$.

Sigamos con $g(K)=H$. Como usaremos las funciones f y g, y la acción de un grupo al mismo tiempo, omitiré los parentesis en la acción del grupo, es decir, si $\sigma \in G \subseteq Aut(E)$ y $\alpha \in E$, escribimos $\sigma\alpha$. Si $K \subseteq E$, escribimos σK.

Como $E \supseteq K$ es Galois, $K = Fix(g(K))$ así que si $\tau \in H$ y $\alpha \in K$, ent $\tau\alpha = \alpha$

Esto implica que para $\sigma \in G$,

$$\sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\tau\alpha = \sigma\alpha$$

i.e., $\sigma\alpha \in F(H^\sigma)$ para todo $\alpha \in K$.

Por lo tanto $\sigma K \subseteq f(H^\sigma)$ y así

$$H^\sigma = gf(H^\sigma) \subseteq g(\sigma K) = Gal(E/\sigma K)$$

Como σ es un automorfismo $[E:K]=[\sigma E:\sigma K]=[E:\sigma K]$. Pero

(ii) $|H^\sigma|=|H|=[E:K]=[E:\sigma K]=|g(\sigma K)|$

Por lo tanto $H^\sigma=g(\sigma K)=Gal(E/\sigma K)$.

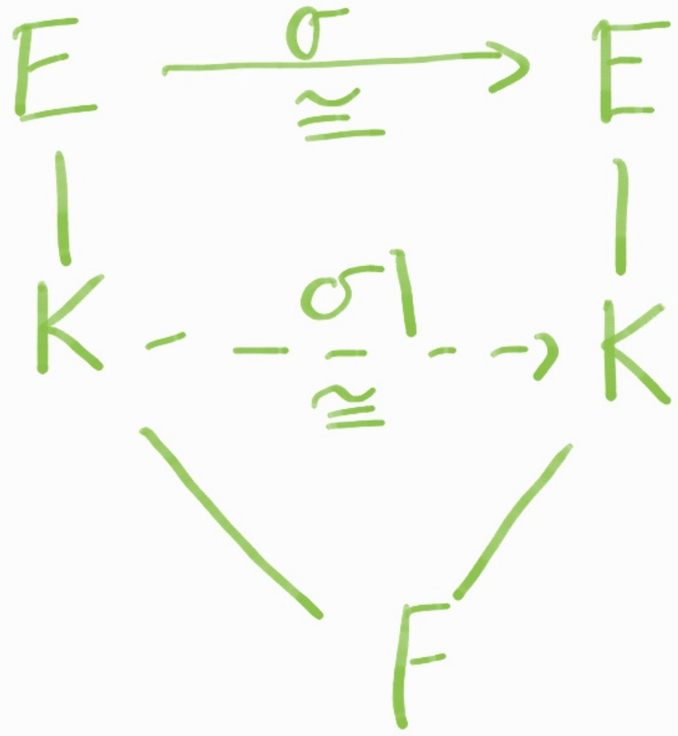
Si $K\supseteq F$ es Galois, entonces $\sigma K=K$ para todo $\sigma\in G$ ya que $K\supseteq F$ es normal

Por lo tanto $H^\sigma=g(\sigma K)=g(K)=H$. Es decir H es normal en G.

Recíprocamente, si $H\triangleleft G$, para cada $\sigma\in G$

$g(K)=H=H^\sigma=g(\sigma K)$. Aplicando f

$K=\sigma K$.



la restricción de σ a K, define un automorfismo de K que fija a F

Entonces tenemos un morfismo $\rho : G \longrightarrow Gal(K/F)$ dado por $\rho(\delta) = \sigma|$. Como $\rho(G) \subseteq Gal(K/F)$,

$$F \subseteq f(Gal(K/F)) \subseteq f(\rho(G)) \subseteq f(G) = F$$

Por lo tanto $F = f(Gal(K/F))$ es decir, $K \supseteq F$ es de Galois. Entonces la función f es inyectiva en los subgrupos de $Gal(K/F)$

Por las igualdades anteriores $\rho(G) = Gal(K/F)$

Un automorfismo $\sigma \in Ker\rho$ si y solo si σ fija a K, es decir, $\sigma \in Gal(E/K)$. Así

$$Gal(K/F) \cong G/Gal(E/K) = G/g(K) = G/H$$

Ejemplo: Consideremos $x^4-2 \in \mathbb{Q}[x]$. que es irreducible

Escribamos $\alpha = \sqrt[4]{2}$, es la unica raiz positiva de f en $\mathbb{R}$. Todas las raices de f son $\alpha, -\alpha, \alpha i$ y $-\alpha i$. Podemos ver que todas las raices de f son distintas y por lo tanto f es separable.

Sea E el campo de descomposicion de f.

Notemos $\mathbb{Q}[\alpha] \subsetneq E$ pero $\alpha i \notin \mathbb{Q}[\alpha] \subseteq \mathbb{R}$.

Por otro lado $i = \frac{\alpha i}{\alpha} \in E$, así que $\mathbb{Q}[\alpha, i] \subseteq E$

De hecho $E = \mathbb{Q}[\alpha, i]$

Como $f = \min_{\mathbb{Q}}(\alpha)$, $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 4$

$$[\mathbb{Q}[\alpha,i]:\mathbb{Q}] = [\mathbb{Q}[\alpha,i]:\mathbb{Q}[\alpha]][\mathbb{Q}[\alpha]:\mathbb{Q}]$$

Sabemos que i es una raiz del polinomio $x^2+1 \in \mathbb{Q}[\alpha][x]$ por lo tanto $\min_{\mathbb{Q}[\alpha]}(i) \mid x^2+1$ en $\mathbb{Q}[\alpha]$. Por lo tanto $[\mathbb{Q}[\alpha,i]:\mathbb{Q}[\alpha]] \leq 2$. Como $\mathbb{Q}[\alpha,i] \neq \mathbb{Q}[\alpha]$ $[\mathbb{Q}[\alpha,i]:\mathbb{Q}[\alpha]] = 2$. Por lo tanto

$[\mathbb{Q}[\alpha,i]:\mathbb{Q}]=8$

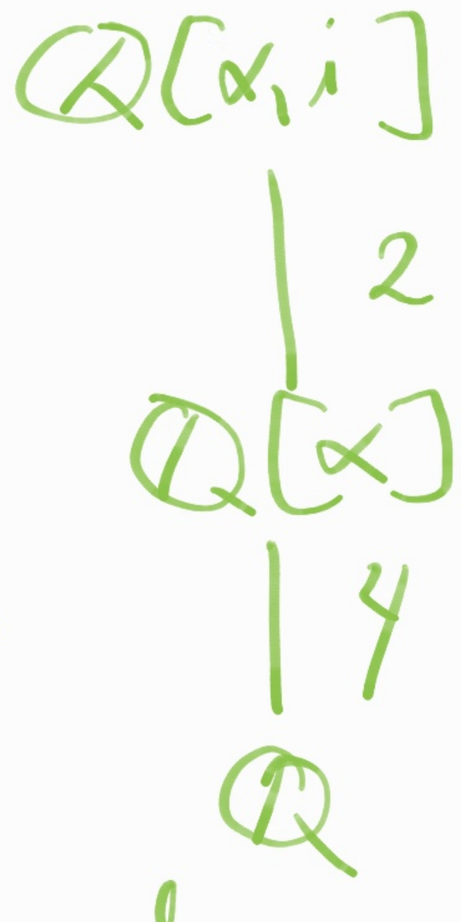
Sea $G=Gal(\mathbb{Q}[\alpha,i]/\mathbb{Q})$. Entonces

$|G|=8$. La extensión $\mathbb{Q}[\alpha]\supseteq\mathbb{Q}$

no es normal, así que el

subgrupo $Hig(\mathbb{Q}[\alpha])$ que le corresponde

no es normal en G.



Salvo isomorfismo solo hay un grupo de orden 8 que tiene un subgrupo no normal de orden 2.

Por lo tanto $G \cong D_8$. Podemos determinar las 8 permutaciones del conjunto $\{\alpha_1, -\alpha_1, \alpha_i, -\alpha_i\}$
La conjugación compleja determina un $\mathbb{Q}$-isomorfismo de E en E, que llamamos τ
Entonces $\tau \in G$ y $\tau(\alpha_i) = -\alpha_i$. En notación de permutación $\tau = (\alpha_i, -\alpha_i)$

Como G actua transitivamente en las raices, existe $\sigma \in G$ tal que $\sigma\alpha = \alpha_i$
Por otro lado, $\sigma(i)$ tiene que ser raiz

del polinomio X^2+1. Por lo tanto $\sigma(i)=\pm i$
Remplazando σ por $\sigma\tau$ si es necesario,
podemos suponer que $\sigma(i)=i$.
$\sigma(\alpha i)=\sigma(\alpha)i=(\alpha i)i=-\alpha$. Entonces la
permutacion inducida por σ es el 4-ciclo
$(\alpha\ \alpha i\ -\alpha\ -\alpha i)$.. Entonces $\langle\sigma\rangle$ es un
subgrupo de orden 4 y $\tau\notin\langle\sigma\rangle$. Así
$G=\langle\sigma,\tau\rangle$

Ahora veamos los campos intermedios. Vamos a ver que $\sqrt{2}, , i, \sqrt{2}i$ están en E y que los campos $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[i],$ y $\mathbb{Q}[\sqrt{2}i]$ son campos intermedios. Notemos que $\mathbb{Q}[\sqrt{2}]$ está contenido en $\mathbb{R}$. y por lo tanto es distinto a los otros dos. Tambien $\mathbb{Q}[i] \neq \mathbb{Q}[\sqrt{2}i]$, ya que de lo contrario $\frac{\sqrt{2}i}{i} = \sqrt{2} \in \mathbb{Q}[i]$ y entonces $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[i]$!.

Entonces hemos encontrado tres diferentes campos intermedios de grado 2 sobre $\mathbb{Q}$

Como $D_8 \cong 6$ tiene exactamente 3 subgrupos de indice 2, $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}i]$ son todos los campos intermedios de grado 2 sobre $\mathbb{Q}$.

Ahora, tendriamos que calcular los K

tal que $[K:\mathbb{Q}]=4$. Dq tiene exactamente cinco subgrupos de orden 2. Por lo tanto hay 5 campos intermedios de orden 4 sobre $\mathbb{Q}$:

$$\mathbb{Q}[\alpha], \mathbb{Q}[i\alpha], \mathbb{Q}[\sqrt{2}, i]$$

$$\mathbb{Q}[\alpha+i\alpha], \quad \mathbb{Q}[\alpha-i\alpha]$$