Subgrupos normales y extensiones normales

Facultad de Ciencias UNAM

Introducción

El objetivo de esta sección es demostrar un par de resultados que serán muy útiles en el futuro.

Para esto, necesitamos un par de recordatorios de teoría de grupos: Supongamos que G es un grupo.

- Si $g \in G$ y $H \leq G$, entonces el conjugado de H por g es el subgrupo

$$gHg^{-1} = \left\{ ghg^{-1} \mid h \in H \right\}$$

- Si $H \leq G$, decimos que H es normal en G si y solo si

$$\forall g \in G \; \forall h \in H \; \left(ghg^{-1} \in H \right)$$

  Equivalentemente $gHg^{-1} \subset H$ para toda $g \in G$. Cabe recalcar que esto ultimo *también* es equivalente a que $gHg^{-1} = H$ para toda $g \in G$.

El conjugado de un campo intermedio

Definición

Supongamos que F, K, L son campos tales que $F \subset K \subset L$. Si $\sigma \in \mathrm{Gal}(L/F)$, decimos que

$$\sigma K := \{\sigma(\alpha) \mid \alpha \in K\}$$

es un **campo conjugado de** K.

Claramente, σK es igual a $\sigma(K)$ (la imagen directa de K bajo σ) pero introducimos esta notación por brevedad. También notemos que como σ es un isomorfismo, σK es un subcampo de L, esto justifica el nombre de "*campo* conjugado".

$[K : F] = [\sigma K : F]$

Lema 1

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si $\sigma \in \mathrm{Gal}(L/F)$, entonces $F \subset \sigma K \subset L$ y $[K : F] = [\sigma K : F]$.

Demostración. La inclusión $\sigma K \subset L$ es clara y la inclusión $F \subset \sigma K$ es consecuencia inmediata de que $\beta = \sigma(\beta)$ para toda $\beta \in F$ (pues $\sigma \in \mathrm{Gal}(L/K)$).

Ahora, veamos que $[K : F] = [\sigma K : F]$. Para esto, recordemos que (por definición), $[K : F]$ es la dimensión de K cuando lo consideramos como F-espacio vectorial. Por eso, para ver que $[K : F] = [\sigma K : F]$, basta demostrar que K y σK son F-espacios vectoriales isomorfos. Usando el hecho de que $\sigma \in \mathrm{Gal}(L/K)$, el lector podrá fácilmente verificar que $\sigma \restriction_K$ es el isomorfismo (entre F-espacios vectoriales) buscado.

$\mathrm{Gal}(L/\sigma K) = \sigma\,\mathrm{Gal}(L/K)\sigma^{-1}$

Lema 2

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si $\sigma \in \mathrm{Gal}(L/F)$, entonces $\mathrm{Gal}(L/\sigma K) = \sigma\,\mathrm{Gal}(L/K)\sigma^{-1}$

Demostración.

$\supset$) Supongamos que $\gamma \in \sigma\,\mathrm{Gal}(L/K)\sigma^{-1}$. Entonces $\gamma = \sigma\tau\sigma^{-1}$ para algún $\tau \in \mathrm{Gal}(L/K)$. Para ver que $\gamma \in \mathrm{Gal}(L/\sigma K)$ necesitamos ver que γ fija a σK. Por eso, supongamos que $\beta \in \sigma K$. Entonces $\beta = \sigma(\alpha)$ para algún $\alpha \in K$ y por lo tanto,

$$\gamma(\beta) = \left(\sigma\tau\sigma^{-1}\right)(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha) = \beta.$$

$\subset$) Supongamos que $\gamma \in \mathrm{Gal}(L/\sigma K)$. Para ver que $\gamma \in \sigma\,\mathrm{Gal}(L/K)\sigma^{-1}$ necesitamos ver que $\gamma = \sigma\tau\sigma^{-1}$ para algún $\tau \in \mathrm{Gal}(L/K)$. Es fácil verificar (de manera análoga a la inclusión anterior) que $\tau \coloneqq \sigma^{-1}\gamma\sigma$ cumple lo deseado.

$\square$

$K = \sigma K \ \forall \sigma \in \mathrm{Gal}(L/F) \iff \mathrm{Gal}(L/K) \lhd \mathrm{Gal}(L/F)$

Proposición 3

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si L/F es una extensión de Galois, entonces

$$K = \sigma K \text{ para toda } \sigma \in \mathrm{Gal}(L/F) \iff \\ \mathrm{Gal}(L/K) \text{ es un subgrupo normal de } \mathrm{Gal}(L/F)$$

Demostración.

$\Longrightarrow$) Si $K = \sigma K$ para toda $\sigma \in \mathrm{Gal}(L/F)$, entonces por el lema 2

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(L/\sigma K) = \sigma \,\mathrm{Gal}(L/K)\sigma^{-1} \text{ para toda } \sigma \in \mathrm{Gal}(L/F).$$

Es decir, $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$.

$\Longleftarrow$) Si $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$, entonces

$$\mathrm{Gal}(L/K) = \sigma\,\mathrm{Gal}(L/K)\sigma^{-1} = \mathrm{Gal}(L/\sigma K) \text{ para toda } \sigma \in \mathrm{Gal}(L/F). \qquad (1)$$

donde la segunda igualdad se cumple por el lema 2.

Por otro lado, como (i) L/F es de Galois (por hipótesis), (ii) $F \subset K \subset L$ (también por hipótesis), y (iii) $F \subset \sigma K \subset L$ (por el lema 1), entonces por el corolario 2.21.10 tenemos que L/K y $L/\sigma K$ son extensiones de Galois. Por lo tanto,

$$K = L_{\mathrm{Gal}(L/K)} = L_{\mathrm{Gal}(L/\sigma K)} = \sigma K \text{ para toda } \sigma \in \mathrm{Gal}(L/F).$$

Donde la segunda igualdad se cumple por (1).

$\square$

Proposición 4

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si L/F es una extensión de Galois, entonces

$$K = \sigma K \text{ para toda } \sigma \in \mathrm{Gal}(L/F) \iff K/F \text{ es normal.}$$

Demostración.

$\Longrightarrow$) Supongamos que $f(x) \in F[x]$ es irreducible en $F[x]$ y que $\alpha \in K$ es una raíz de $f(x)$. Entonces existe $c \in F$ tal que $f(x) = c \cdot m_{\alpha,F}(x)$. Mas aun, como L/F es Galois, entonces corolario 2.21.8

$$f(x) = c \cdot m_{\alpha,F}(x) = c \cdot \prod_{i=1}^{n}(x - \alpha_i)$$

donde $\alpha_1, \ldots, \alpha_n$ son los distintos elementos de $\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(L/F)\}$.

$\Longleftarrow$) Supongamos que K/F es normal. Empecemos por ver que $\sigma K \subset K$ para toda $\sigma \in \mathrm{Gal}(L/F)$. Sea $\sigma \in \mathrm{Gal}(L/F)$ y $\beta \in \sigma K$, es decir $\beta = \sigma\alpha$ para alguna $\alpha \in K$. Ahora bien, como $\sigma \in \mathrm{Gal}(L/F)$, entonces (por la proposición 2.18.4) tenemos que $\beta = \sigma\alpha$ es raíz de $m_{\alpha,F}(x)$. Pero $m_{\alpha,F}(x)$ es un polinomio irreducible en $F[x]$ que tiene una raíz en K y por lo tanto, como K/F es normal, entonces $m_{\alpha,F}(x)$ se descompone en K/F. Como β es raíz de $m_{\alpha,F}(x)$, lo anterior implica que $\beta \in K$.

$\square$

Una equivalencia muy importante para los campos intermedios de una extensión de Galois

Teorema 5

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si L/F es una extensión de Galois, entonces las siguientes condiciones son equivalentes

1. $K = \sigma K$ para toda $\sigma \in \mathrm{Gal}(L/F)$.
2. $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$.
3. K/F es una extensión de Galois.
4. K/F es una extensión normal.

Demostración. La proposición 3 demuestra precisamente que (1) $\iff$ (2) y la proposición 4 que (1) $\iff$ (4). Para concluir, veamos que (3) $\iff$ (4). Obviamente, (3) $\implies$ (4). Conversamente, resta probar que K/F es separable. Sin embargo, esto es consecuencia inmediata de que $F \subset K \subset L$ y de que L/F es separable (pues por hipótesis es de Galois). $\square$

$\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F)$

Teorema 6

Supongamos que F, L, K son campos tales que $F \subset K \subset L$. Si L/F y K/F son de Galois, entonces

$$\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F).$$

Demostración. Antes que nada, notemos que el cociente $\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K)$ es un grupo bien definido porque la hipótesis K/F es Galois implica (por el teorema anterior) que $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$.

Como has de esperar, para demostrar $\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F)$ encontraremos un homomorfismo suprayectivo de $\mathrm{Gal}(L/F)$ en $\mathrm{Gal}(K/F)$ con kernel igual a $\mathrm{Gal}(L/K)$. Usando esto, el primer teorema de isomorfismos de grupos implicara lo deseado.

Considera

$$\begin{aligned}\phi : \mathrm{Gal}(L/F) &\to \mathrm{Gal}(K/F)\\ \sigma &\mapsto \sigma \restriction_K\end{aligned}$$

- *ϕ esta bien definido*:

  Específicamente, queremos ver que si $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma \restriction_K$ (su restricción a K) pertenece a $\mathrm{Gal}(K/F)$. Claramente, $\sigma \restriction_K$ fija a F y por lo tanto, basta probar que $\sigma \restriction_K$ es un automorfismo de K.

  Para esto, notemos que como σ es un automorfismo de L, entonces $\sigma \restriction_K$ es un isomorfismo de K en su imagen, σK. Sin embargo, la hipótesis K/F es de Galois implica (por el teorema anterior) que $K = \sigma K$ para toda $\sigma \in K$. Por lo tanto, $\sigma \restriction_K$ es un isomorfismo de K en $\sigma K = K$, es decir, $\sigma \restriction_K$ es un automorfismo de K.

- *ϕ es un homomorfismo*:

  En el inciso anterior demostramos que si $\sigma \in \mathrm{Gal}(L/F)$, entonces $\sigma \restriction_K$ es una función de K en K. Es fácil verificar que esto implica que, $(\sigma \circ \tau) \restriction_K = \sigma \restriction_K \circ \tau \restriction_K$ para toda $\sigma, \tau \in \mathrm{Gal}(L/F)$. Escribiendo esto en términos de ϕ obtenemos $\phi\,(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau)$, es decir, ϕ es un homomorfismo.

- *El kernel de ϕ es* $\operatorname{Gal}(L/K)$:

  Si $\sigma \in \operatorname{Gal}(L/F)$, entonces

$$\sigma \in \ker \phi \iff \phi(\sigma) = \mathrm{id}_K \iff \sigma \restriction_K = \mathrm{id}_K \iff \sigma \in \operatorname{Gal}(L/K).$$

- *ϕ es suprayectivo*:

  Los incisos anteriores y el primer teorema de isomorfismos de grupos implican que $\operatorname{Gal}(L/F)/\operatorname{Gal}(L/K) \cong \operatorname{im}\phi$. Usando esto obtenemos la primera de las siguientes igualdades

$$\begin{aligned}
|\operatorname{im}\phi| &= \big|\operatorname{Gal}(L/F)/\operatorname{Gal}(L/K)\big| \\
&= \frac{\big|\operatorname{Gal}(L/F)\big|}{\big|\operatorname{Gal}(L/K)\big|} && \text{(por el teorema de Lagrange)} \\
&= \frac{[L:F]}{[L:K]} && \text{(porque } L/F \text{ y } L/K \text{ son de Galois)} \\
&= [K:F] && \text{(porque } [L:F] = [L:K][K:F]\text{)} \\
&= \big|\operatorname{Gal}(K/F)\big| && \text{(porque } K/F \text{ es de Galois)}
\end{aligned}$$

  Como $\operatorname{im}\phi \subset \operatorname{Gal}(K/F)$ y $\operatorname{Gal}(K/F)$ es finito, la igualdad anterior implica que $\operatorname{im}\phi = \operatorname{Gal}(K/F)$.

$\sigma F(\alpha) = F(\sigma\alpha)$

Lema 7

Supongamos que M/F es una extensión de campos. Si $\alpha \in M$ y $\sigma \in \mathrm{Gal}(M/F)$, entonces $\sigma F(\alpha) = F(\sigma\alpha)$.

Demostración. Antes que nada, recordemos que en el corolario 2.5.2 demostramos que si $n = \deg m_{\alpha,F}(x)$, entonces

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

es una F-base de $F(\alpha)$.

Por otro lado, como $\sigma \in \mathrm{Gal}(M/F)$, entonces la proposición 2.18.4 implica que $m_{\alpha,F}(x) = m_{\sigma\alpha,F}(x)$ y por lo tanto, (por el corolario 2.5.2) también tenemos que

$$\{1, \sigma\alpha, (\sigma\alpha)^2, \ldots, (\sigma\alpha)^{n-1}\}$$

es una F-base de $F(\sigma\alpha)$.

Usando esto y la definición de $\sigma F(\alpha)$, es fácil obtener lo deseado. $\square$

Si L es un campo intermedio de la extensión de Galois M/F, entonces el producto de todos los campos conjugados de L es la cerradura de Galois de L/F

Proposición 8

Supongamos que F, L, M son campos tales que $F \subset L \subset M$. Si M/F es una extensión de Galois, entonces el producto de todos los campos conjugados de L es la cerradura de Galois de L/F. Específicamente, si

$$\mathrm{Gal}(M/F) = \{\sigma_1, \sigma_2 \ldots, \sigma_n\},$$

entonces

$$(\sigma_1 L)(\sigma_2 L) \cdots (\sigma_n L)$$

es la cerradura de Galois de L/F.

Demostración. Supongamos que $F \subset L \subset M$ y que M/F es de Galois. En particular, M/F es finita separable y por lo tanto (como $F \subset L \subset M$), L/F también es finita separable. Por el teorema del elemento primitivo, lo anterior implica que $L = F(\alpha)$ para alguna $\alpha \in L$.

Ahora bien, como M/F es normal (pues es de Galois) y $\alpha \in L \subset M$, entonces el polinomio mínimo de α sobre F se descompone en M/F. Entonces, podemos escribir

$$m_{\alpha,F}(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r) \text{ con } \alpha_1 = \alpha \text{ y } \alpha_2, \ldots, \alpha_r \in M.$$

En lo que sigue, veremos que $F(\alpha_1, \ldots, \alpha_r)$ es la cerradura de Galois de L/F.

Primero, notemos que $m_{\alpha_i,F}(x) = m_{\alpha,F}(x)$ para toda $i \in \{1, \ldots, r\}$ y en particular,

$$\{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\} = \{m_{\alpha,F}(x)\}.$$

Por lo tanto, la proposición 2.20.1 (la de la existencia de cerraduras de Galois) implica que el campo de descomposición de $m_{\alpha,F}(x)$ sobre L es la cerradura de Galois de L/F. Cabe recalcar que para poder ocupar este resultado es necesario observar que $L = F(\alpha)$ y que α es separable.

Pero como

$$m_{\alpha,F}(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r),$$

entonces el campo de descomposición de $m_{\alpha,F}(x)$ sobre L es $F(\alpha_1,\ldots,\alpha_r)$. Por lo tanto, $F(\alpha_1,\ldots,\alpha_r)$ es la cerradura de Galois de L/F.

Finalmente, notemos que

$$\begin{aligned}
(\sigma_1 L)(\sigma_2 L)\cdots(\sigma_n L) &= \big(\sigma_1 F(\alpha)\big)\big(\sigma_2 F(\alpha)\big)\cdots\big(\sigma_n F(\alpha)\big) \\
&= \big(F(\sigma_1\alpha)\big)\big(F(\sigma_2\alpha)\big)\cdots\big(F(\sigma_n\alpha)\big) \\
&\qquad\qquad\qquad\qquad\qquad \text{(por el lema anterior)} \\
&= F(\alpha_1)\cdots F(\alpha_r) \\
&= F(\alpha_1,\ldots,\alpha_r) \qquad\qquad \text{(por el corolario 2.8.2)}
\end{aligned}$$

Donde la tercera igualdad se cumple porque (i) toda α_i es de la forma $\sigma_j\alpha$ para alguna $\sigma_j \in \mathrm{Gal}(M/F)$ y (ii) el producto de un subcampo consigo mismo es el mismo, es decir $KK = K$.

Por lo tanto, $(\sigma_1 L)(\sigma_2 L)\cdots(\sigma_n L)$ es la cerradura de Galois de L/F. $\square$