# TAREA ÁLGEBRA MODERNA
# SEMESTRE 2013-II
# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
# HÉCTOR MANUEL TÉLLEZ GÓMEZ

## Proposición 11

**Lema 1** *Sea $H$ un grupo cíclico y sea $N$ un grupo arbitrario. Si $\varphi$ and $\psi$ son monomorfismos de $H$ a $Aut(N)$ tales que $\varphi(H) = \psi(H)$, entonces $N \rtimes_\varphi H \cong N \rtimes_\psi N$.*

**Demostración:** Sea $H =< x >$. Como las imágenes de $H$ bajo $\varphi$ y $\psi$, $\varphi(x)$ y $\psi(x)$ generan al mismo subgrupo cícilco de $Aut(N)$. Por lo tanto existen $a, b \in \mathbb{Z}$ tales que $\varphi(x)^a = \psi(x)$ y $\varphi(x) = \psi(x)^b$.

De aquí que:

$$\varphi(x) = \psi(x)^b = \varphi(x)^{ab} = \varphi(x^{ab}).$$

Como $\varphi$ es monomorfimso, tenemos que

$$x = x^{ab} \tag{1}$$

Es decir, elevar a la $ab$ es otra manera de escribir el homomorfismo identidad.

Como $H$ es cíclico tenemos que para todo $h \in H$, existe $r \in \mathbb{Z}$ tal que $x^r = h$ y entonces

$$\varphi(h^a) = \varphi((x^r)^a) = \varphi(x^a r) = (\varphi(x)^a)^r = \psi(x)^r = \psi(x^r) = \psi(h),$$

análogamente $\varphi(h) = \psi(h^b)$.

Definamos $\tau : N \rtimes_\varphi H \to N \rtimes_\psi N$ como $\tau(n, h) = (n, h^a)$.

$$\begin{aligned}
\tau((n_1, h_1)(n_2, h_2)) &= \tau(n_1\psi(h_1)(n_2), h_1h_2) \\
&= (n_1\psi(h1)(n_2), (h_1h_2)^a) \\
&= (n_1\varphi(h_1^a)(n_2), h_1^a h_2^a) \\
&= n_1h_1^a n2h_2^a \text{ (por definición de } N \rtimes_\psi H) \\
&= \tau(n_1h_1)\tau(n_2h_2)
\end{aligned}$$

Con esto, tenemos que $\tau$ separa productos y manda inversos en inversos. Por lo tanto $\tau$ es homomorfismo.

Análogamente $\lambda : N \rtimes_\psi H \to N \rtimes_\varphi N$ definida como $\lambda(n,h) = (n,h^b)$, resulta ser homomorfismo.

Ahora notemos que $\tau \circ \lambda(n,h) = \tau(n,h^b) = (n,h^{ab})$ y por (1), tenemos que $\tau \circ \lambda = id_{N \rtimes_\psi H}$.

Análogamente, tenemos que $\lambda \circ \tau = id_{N \rtimes_\varphi H}$. Con esto tenemos que tanto $\tau$ como $\lambda$ son isomorfismos, con lo que termina la demostración.

## Proposición 12

**Lema 2** *Sean $N$ y $H$ grupos, sea $\psi : H \to Aut(N)$ un homomorfismo y $f \in Aut(N)$. Si $\hat{f}$ es el automorfismo interno de $Aut(N)$ inducido por $f$, entonces $N \rtimes_{\hat{f}\circ\psi} \cong N \rtimes_{\psi} H$.*

**Demostración:** Sea $\theta : N \rtimes_{\psi} H \to N \rtimes_{\hat{f}\circ\psi}$ definida por $\theta(n,h) = (f(n),h)$. Veamos que $\theta$ es homomorfismo:

$$\begin{aligned}
\theta((n_1,h_1)\cdot(n_2,h_2)) &= \theta(n_1\psi(h_1)(n_2), h_1h_2)\\
&= (f(n_1\psi(h_1)(n_2)), h_1h_2)\\
&= (f(n_1)\cdot(f\circ\psi(h_1))(n_2), h_1h_2)\\
&= (f(n_1)\cdot(f\circ\psi(h_1)\circ f^{-1}\circ f)(n_2), h_1h_2)\\
&= (f(n_1)\cdot(\hat{f}(\psi(h_1))\circ f)(n_2), h_1h_2)\\
&= (f(n_1)\cdot(\hat{f}\circ\psi)(h_1)f(n_2), h_1h_2)\\
&= (f(n_1),h_1)(f(n_2),h_2)\\
&= \theta(n_1,h_1)\theta(n_2,h_2).
\end{aligned}$$

Con esto hemos demostrado que $\theta$ es homomorfismo pues abre multiplicaciones y manda inversos en inversos.

De manera análoga vemos que $\iota : N \rtimes_{\hat{f}\circ\psi} \to N \rtimes_{\psi} H$ definida por $\iota(n,h) = (f^{-1}(n),h)$ es homomorfismo.

Ahora notemos que:

$$(\iota\circ\theta)(n,h) = \iota(f(n),h) = (f^{-1}(f(n)),h) = (n,h).$$

Por lo tanto $\iota\circ\theta = id_{N\rtimes_{\psi}H}$.

Análogamente $\theta\circ\iota = id_{N\rtimes_{\hat{f}\circ\psi}H}$. Por lo tanto, $\theta$ y $\iota$ son isomorfismos y con esto terminamos la demostración.

## Schur-Zassenhaus

Antes de continuar con la demostración del teorema de Schur-Zassenhaus, nececitaremos algunas definiciones.

**Definición 1** *Decimos que $H$ es* ***complemento de un subgrupo normal*** *$N$ de $G$, si $H \subset G$ y $G = N \rtimes H$.*

**Definición 2** *Decimos que un subgrupo $H$ de un grupo finito $G$ es un* ***subgrupo de Hall*** *si $([G:H], |H|) = 1$.*

**Teorema 3** (Teorema de Schur-Zassenhaus) *Todo subgrupo normal de Hall tiene complemento.*

**Demostración:** Sea $Nn$ un subgrupo normal de Hall de un grupo finito $G$. Si $G$ tiene un subgrupo $K$ de orden $n = [G : N]$, entonces tenemos que $N \cap K = 1$ gracias al teorema de Lagrange, pues $n$ y $|N|$ son primos relativos. Entonces

$$\begin{aligned} |NK| &= \frac{|N||K|}{|N \cap K|} \\ &= |N||K| \\ &= |G| \end{aligned}$$

y por lo tanto $K$ es un complemento de $G$.

Entonces, sería suficiente probar que $G$ siempre tiene un subgrupo de orden $n$. Para ello procederemos por inducción suponiendo que todo grupo finito de orden menor que $|G|$ que contenga un subgrupo normal de Hall, también tiene un subgrupo cuyo orden es igual al índice de dicho subgrupo.

Sea $P$ un subgrupo de Sylow de $N$. El argumento de Frattini nos dice que $G = N_G(P)N$.

Ahora, $N_N(P) = N_G(P) \cap N$, pues $N_N(P) = \{g \in N | gP = Pg\}$, y $N_G(P) = \{g \in G | gP = Pg\}$. es decir si $g_0 \in N_G(P) \cap N$ quiere decir que $g_0 \in N$ y que $g_0 P = P g_0$. Esto demuestra una de las contenciones y la restante es igual de fácil. Ahora, también tenemos que $N_G(P) \cap N \trianglelefteq N_G(P)$, pues si $g \in N_G(P) \cap N$ y $h \in N_G(P)$, por un lado $hgh^{-1} \in N$ gracias a que $g \in N$ y que $N$ es normal en $G$, y por otro lado $hgh^{-1} \in N_G(P)$, pues $N_G(P)$ es un subgrupo y tanto $g$ como $h$ son elementos de él.

Ahora, por las equivalencias recién dadas y por el segundo teorema de isomorfismos (el segundo según la numeración de J. Rotman) tenemos lo siguiente:

$$\begin{aligned}
\frac{G}{N} &= \frac{N_G(P)N}{N} \\
&\cong \frac{N_G(P)}{N_G(P) \cap N} \\
&= \frac{N_G(P)}{N_N(P)}
\end{aligned}$$

## Dedekind

Antes de comenzar con la demostración del Lema de Dedekind, haremos algunas definiciones.

**Definición 4** *Un **caracter** de un grupo $G$ en un campo $E$ es un homomofrphismo de grupos*

$$\sigma : G \longrightarrow E^{\#}$$

*Donde $E^{\#} = E - \{0\}$ es el grupo multiplicativo de $E$.*

**Definición 5** *Un conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ de caracteres de un grupo $G$ en un campo $E$ es **independiente** si no existen $a_1, a_2, \ldots, a_n \in E$, no todos 0, tales que*

$$\sum a_i \sigma_i(x) = 0 \quad \forall x \in G$$

Ahora estamos listos para el Lema de Dedekind.

**Lema 3** (Dedekind) *Todo conjunto $\{\sigma_1, \ldots, \sigma_n\}$ de caracteres distintos de un grupo $G$ en un campo $E$ es independiente.*

**Demostración:** Procedemos por inducción sobre $n$.

- Base de inducción

  Sea $n = 1$. Si $\{\sigma_1\}$ no fuera independiente entonces existiría $a_1 \in E$, con $a_1 \neq 0$ tal que $a_1\sigma_1(x) = 0$. Pero tanto $a_1$ como $\sigma_1(x)$ son distintos de 0 y pertenecen a un campo (es decir, a un dominio entero) y por lo tanto no es posible que $a_1\sigma_1(x) = 0$.

- Hipótesis de inducción

  Sea $n > 1$. Y supongamos que para $m < n$ se cumple el resultado.

- Paso inductivo

  Supongamos que existen $a_1, \ldots, a_n \in E$ tales que para todo $x \in G$ se tiene que

$$\sum a_i \sigma_i(x) = 0 \tag{2}$$

Por hipótesis de inducción, tenemos que $a_1, \ldots, a_n$ son necesariamente todos distintos de cero. También podemos suponer que $a_n = 1$, si no es así, basta multiplicar la suma por $a_n^{-1}$.

Como $\sigma_n \neq \sigma_1$, necesariamente existe $y \in G$ tal que $\sigma_n(y) \neq \sigma_1(y)$. Como (2) aplica para todo $x \in G$, en particular aplica para $yx$. Entonces tenemos que

$$\begin{aligned} \sum a_i\sigma_i(yx) &= \sum a_i\sigma_i(y)\sigma_i(x) \\ &= 0 \end{aligned}$$

Multiplicando esto por $\sigma_n(y)^{-1}$ y, recordando que $a_n = 1$, obtenemos

$$\begin{aligned} \sigma_n(y)^{-1}\sum a_i\sigma_i(y)\sigma_i(x) &= \sum a_i\sigma_n(y)^{-1}\sigma_i(y)\sigma_i(x) \\ &= \sum_{i<n} a_i\sigma_n(y)^{-1}\sigma_i(y)\sigma_i(x) + \sigma_n(x) \\ &= 0. \end{aligned}$$

Restando esto último de (2) obtenemos

$$\begin{aligned} \sum_{i<n} a_i\sigma_i(x) + \sigma_n(x) - (\sum_{i<n} a_i\sigma_n(y)^{-1}\sigma_i(y)\sigma_i(x) + \sigma_n(x)) \\ = \sum_{i<n} a_i\sigma_i(x) - a_i\sigma_n(y)^{-1}\sigma_i(y)\sigma_i(x) \\ = \sum_{i<n} a_i(1 - \sigma_n(y)^{-1}\sigma_i(y))\sigma_i(x) \\ = 0. \end{aligned}$$

Por un lado, la hipótesis de inducción nos dice que esto es cierto sólamente si $a_i(1-\sigma_n(y)^{-1}\sigma_i(y)) = 0$ para todo $i$. En particular para $i = 1$ tendríamos $a_1(1 - \sigma_n(y)^{-1}\sigma_1(y)) = 0$. Como $a_1 \neq 0$ esto obliga a $\sigma_n(y)^{-1}\sigma_1(y) = 1$, y por lo tanto $\sigma_n(y) = \sigma_1(y)$, lo cual contradice nuestra elección de $y$.

Y con esto hemos demostrado que no existen tales $a_1, \ldots, a_n$.

## Artin

Comenzaremos por hacer las definiciones pertinentes.

**Definición 6** *Sea $Aut(E)$ el grupo de todos los automorfismos de un campo $E$. Si $G \subset Aut(E)$, entonces a*

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha paratodo \sigma \in G\}$$

*se le llama el* ***campo fijo****.*

Antes de pasar a la demostracióndе del teorema de Artin, enunciaremos sin demostración un lema que nos será de utilidad.

**Lema 4** *Si $G = \{\sigma_1, \ldots, \sigma_n\} \subset Aut(E)$, entonces*

$$[E : E^G] \geq n$$

**Teorema 7** (Artin) *Si $G = \{\sigma_1, \ldots, \sigma_n\} \leq Aut(E)$, entonces:*

$$[E : E^G] = |G|$$

**Demostración:** Gracias a [4] sólo hace falta demostrar que no es posible que $[E : E^G] > n$. Supongamos esto cierto.

Esto significa que existe un conjunto con al menos $n+1$ elementos linealmente independientes en $E$ como $E^G$-espacio vectorial. Sean $\{\omega_1, \ldots, \omega_{n+1}\}$.