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 φ and ψ 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 φ y ψ, $\varphi(x)$ 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 φ 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 $\tau(n, h) = (n, h^a)$.

$$\begin{aligned}
\tau((n_1, h_1)(n_2, h_2)) &= \tau(n_1\psi(h_1)(n_2), h_1h_2) \\
&= (n_1\psi(h1)(n_2), (h_1h_2)^a) \\
&= (n_1\varphi(h_1^a)(n_2), h_1^a h_2^a) \\
&= n_1 h_1^a n2 h_2^a \text{ (por definición de } N \rtimes_\psi H) \\
&= \tau(n_1h_1)\tau(n_2h_2)
\end{aligned}$$

Con esto, tenemos que τ separa productos y manda inversos en inversos. Por lo tanto τ 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 τ como λ 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 θ 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 θ 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, θ y ι 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 N 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:

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

Entonces $[N_G(P) : N_N(P)] = n$. Como $N_N(P) \subset N$, tenemos que $|N_N(P)|$ divide a $|N|$ y por lo tanto $(|N_N(P)|, n) = 1$. Es decir que $N_N(P)$ es un subgrupo normal de Hall del $N_G(P)$.

Si $N_G(P) < G$, entonces, por hipótesis de inducción $N_G(P)$, y entonces G tiene un subgrupo de orden n. Entonces falta el caso en el que $N_G(P) = G$, o equivalentemente, que $P \trianglelefteq G$.

Supongamos entonces que $P \trianglelefteq G$ y analizaremos el caso en el que $P \triangleleft N$ (contención propia). Por el teorema de la correspondencia, tenemos que $\frac{N}{P} \trianglelefteq \frac{G}{P}$ y que $|\frac{G}{P} : \frac{N}{P}| = |G : N| = n$. Como $|\frac{N}{P}|$ divide a $|N|$ y $|\frac{G}{P}| < |G|$, por inducción, $\frac{G}{P}$ tiene un subgrupo de orden n; este subgrupo debe ser de la forma $\frac{L}{P}$ donde $P \triangleleft L \leq G$. Ahora, $|L \cap N|$ divide a $|L| = n|P|$ y $|N|$. Como $|N|$ y n son primos relativos, eso forza a que $|L \cap N|$ divide a P y por lo tanto $P \leq |L \cap N|$. Pero como $P \subset L \cap N$, concluimos que $P = L \cap N$ y en particular L está contenido propiamente en G. Como $|P|$ y $|\frac{L}{P}| = n$ son primos relativos, por inducción L, y entonces G, tiene un subgrupo de orden n.

Ahora falta el caso en el que $P = N$. Para esto dividiremos en dos subcasos.

Caso 1. Si N es un subgrupo no abeliano de G, entonces, dado que N es un p-grupo, tenemos que $Z = Z(N)$ es un subgrupo propio de N no trivial, y dado que el centro de un grupo es un subgrupo característico, tenemos que $Z \triangleleft G$. Usando el Teorema de la Correspondencia tenemos que $\frac{G}{Z}$ tiene un subgrupo normal $\frac{G}{N}$ de índice n. Por inducción tenemos que $\frac{G}{Z}$ tiene un subgrupo de orden n de la forma $\frac{L}{Z}$, donde $Z \triangleleft L \leq G$. Por lo tanto, de manera análoga a lo hecho previamente, tenemos que $L \cap N = Z$, lo que en particular nos dice que L es un subgrupo propio de G. En este caso se tiene que $|Z|$ y $|\frac{L}{Z}$ son primos relativos, así que, por inducción tenemos que L tiene un subgrupo de orden n, el cual también es un subgrupo de G.

Caso 2. Sea $H = G/A$ y sea $h \in H$. Sean $t, u \in h$, entonces se tiene que $t^{-1}u \in A$ (dado que $tA = uA = h$), y por lo tanto, dado que A es abeliano, tenemos que para todo $x \in A$ se cumple

$$ux \;=\; tt^{-1}ux,$$

$$\begin{aligned} ux &= txt^{-1}u, \\ uxu^{-1} &= txt^{-1}. \end{aligned}$$

Por lo tanto podemos definir una acción de H en A por conjugación, es decir, para cada $h \in H$ y para cada $x \in A$ definimos

$$^{h}x := txt^{-1},$$

y lo demostrado anteriormente nos dice que dicha acción está bien definido. Notemos que para toda $x, y \in A$ y para toda $h \in H$ se tiene que

$$\begin{aligned} ^{h}(xy) &= t(xy)t^{-1} \\ &= t(xt^{-1}ty)t^{-1} \\ &= (txt^{-1})(tyt^{-1}) \\ &= {}^{h}x^{h}y. \end{aligned}$$

Esto nos dice que dicha acción se puede ver como un homomorfismo de H en $Aut(A)$.

Sea $h \in H$ y sea $t_h \in h$. El conjunto $\{t_h : h \in H\}$ es una transversal de A en G que contiene n elementos. Tenemos que para toda $h_1, h_2 \in H$ se cumple

$$\begin{aligned} t_{h_1h_2}^{-1}A &= (t_{h_1h_2}A)^{-1} \\ &= (h_1h_2)^{-1} \\ &= h_2^{-1}h_1^{-1} \\ &= (t_{h_2^{-1}}A)(t_{h_1^{-1}}A), \end{aligned}$$

por lo tanto $t_{h_1}t_{h_2}t_{h_1h_2}^{-1} \in A$. Sea $f : H \times H \to A$ la función definida para $(h_1, h_2) \in H \times H$ por

$$f(h_1, h_2) := t_{h_1}t_{h_2}t_{h_1h_2}^{-1},$$

por lo tanto $f(h_1, h_2)t_{h_1h_2} = t_{h_1}t_{h_2}$. Entonces tenemos que

$$\begin{aligned} t_{h_1}(t_{h_2}t_{h_3}) &= t_{h_1}f(h_2, h_3)t_{h_2h_3} \\ &= (t_{h_1}f(h_2, h_3)t_{h_1}^{-1})t_{h_1}t_{h_2h_3} \\ &= {}^{h_1}f(h_2h_3)f(h_1, h_2h_3)t_{h_1h_2h_3}, \end{aligned}$$

y también

$$\begin{aligned} (t_{h_1}t_{h_2})t_{h_3} &= f(h_1, h_2)t_{h_1h_2}t_{h_3} \\ &= f(h_1, h_2)f(h_1h_2, h_3)t_{h_1h_2h_3}. \end{aligned}$$

Por lo tanto, para todas $h_1, h_2, h_3 \in H$ tenemos que f satisface

$$^{h_1}f(h_2h_3)f(h_1, h_2h_3) = f(h_1, h_2)f(h_1h_2, h_3) \tag{2}$$

Sea $e : H \to A$ la función definida para $h \in H$ por

$$e(h) := \prod_{k \in H} f(h, k).$$

Usando la ecuación (2) tenemos que

$$\begin{aligned} f(h_1, h_2)^n e(h_1 h_2) &= f(h_1, h_2)^n \prod_{h_3 \in H} f(h_1 h_2, h_3) \\ &= \prod_{h_3 \in H} \big(f(h_1, h_2) f(h_1 h_2, h_3) \big) \\ &= \prod_{h_3 \in H} \big({}^{h_1} f(h_2 h_3) f(h_1, h_2 h_3) \big) \\ &= {}^{h_1}\left(\prod_{k \in H} f(h_2, k) \right) \left(\prod_{k \in H} f(h_1, k) \right) \\ &= {}^{h_1} e(h_2) e(h_1). \end{aligned}$$

Por lo tanto, dado que A es abeliano, para todos $h_1, h_2 \in H$ se tiene que

$$\begin{aligned} f(h_1, h_2)^n &= {}^{h_1} e(h_2) e(h_1) e(h_1 h_2)^{-1} \\ &= e(h_1 h_2)^{-1} e(h_1)\, {}^{h_1} e(h_2), \end{aligned}$$

y también que para todas $x, y \in X$ se tiene que $(xy)^n = x^n y^n$, lo que nos dice que la función definida por $x \mapsto x^n$ es un automorfismo, dado que n y $|A|$ son primos relativos. Denotaremos por $\sqrt[n]{x}$ a la preimagen de x bajo dicho automorfismo. Es fácil ver que para toda $x \in A$ se tiene que $\sqrt[n]{xy} = \sqrt[n]{x}\,\sqrt[n]{y}$ y que $\sqrt[n]{x^{-1}} = \sqrt[n]{x}^{-1}$. Sea $c : H \to A$ la función definida para $h \in H$ por

$$c(h) := \sqrt[n]{x}^{-1},$$

por lo tanto, para todas $h_1, h_2 \in H$ se tiene que

$$\begin{aligned} f(h_1, h_2) &= \sqrt[n]{e(h_1 h_2)^{-1} e(h_1)\, {}^{h_1} e(h_2)} \\ &= c(h_1 h_2) c(h_1)^{-1}\, {}^{h_1} c(h_2). \end{aligned}$$

Entonces, tenemos que para todas $h_1, h_2 \in H$ se tiene que

$$\begin{aligned} c(h_1 h_2) t_{h_1 h_2} &= c(h_1)\, {}^{h_1} c(h_2) f(h_1 h_2) t_{h_1 h_2} \\ &= c(h_1) t_{h_1} c(h_2) t_{h_1}^{-1} t_{h_1} t_{h_2} \\ &= c(h_1) t_{h_1} c(h_2) t_{h_2}. \end{aligned}$$

Por lo tanto, la función $\varphi : H \to G$ definida por

$$\varphi(h) := c(h) t_h$$

es un morfismo y, si $h \neq 1$ se tiene que $t_h \notin A$ y por lo tanto $c(h)t_h \neq 1$, así que φ es un monomorfismo de grupos, cuya imagen es un subgrupo de G de orden n.

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

$$\sum a_i \sigma_i(x) = 0 \tag{3}$$

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 (3) 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 (3) 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 $a_1, \ldots, a_n$.

Lema 78

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*

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}$$

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

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

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

Demostración: Supongamos lo contrario, entonces $[E : E^G] = r < n$; sea $\{\alpha_1, \ldots, \alpha_r\}$ una base de E como E^G espacio vectorial. Considere el sistema de r ecuaciones con n incógnitas:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0 \\ &\vdots \\ \sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n &= 0 \end{aligned}$$

Como tenemos menos ecuaciones que incógnitas, existe una solución no tribial $(x_1, \ldots, x_n)$. Para cualqueir $\beta \in E$ existen $b_i \in E^G$, $(1 \leq i \leq r)$ tales que $\beta = \sum b_i \alpha_i$.

Multipliquemos entonces la i-ésima ecuación por b_i para obtener el sistema con i-éxima ecuación:

$$b_i\sigma_1(\alpha_i)x_1 + \cdots + b_i\sigma_n(\alpha_i)x_n = 0$$

Y esto lo podemos reescribir como

$$\sigma(b_i)\sigma_1(\alpha_i)x_1 + \cdots + \sigma(b_i)\sigma_n(\alpha_i)x_n = 0$$

dado que $b_i \in E^G$ y los σ_j fijan a todos los elementos de este conjunto.

Lo anterior también se puede escribir como:

$$\sigma(b_i\alpha_i)x_1 + \cdots + \sigma(b_i\alpha_i)x_n = 0$$

Y sumando todas las ecuaciones del sistema obtenemos:

$$\sigma\left(\sum b_i\alpha_i\right)x_1+\cdots+\sigma\left(\sum b_i\alpha_i\right)x_n = \\ \sigma(\beta)x_1+\cdots+\sigma(\beta)x_n=0.$$

Como $\beta\in E$ fue escogido arbitrariamente, esta última ecuación contradice la independencia de los caracteres $\{\sigma_1,\ldots,\sigma_n\}$.

Artin

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 $\{\omega_1, \ldots, \omega_{n+1}\}$.

Consideremos entonces el sistema de n ecuaciones con $n+1$ incógnitas:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0. \end{aligned} \tag{4}$$

Se trata de un sistema de ecuaciones homogeneo, así que su espacio solución tiene al menos dimensión 1. Es decir, existe una solución no trivial sobre E. Escogemos una solución que tenga el menor número r de componentes cero, digamos $(a_1, \ldots, a_r, 0, \ldots, 0)$, podemos asumir que las entradas no cero están en las primeras r entradas (si no es así, basta reordenar la base).

También podemos asumir que $a_r = 1$, de otra manera basta con multiplicar por su inverso en todas las ecuaciones. Notemos ahora que $r \neq 1$, pues $\sigma_1(\omega_1)a_1 = 0$ implicaría $a_1 = 0$.

Notemos también que no todas las a_i pertenecen a E^G. De lo contrario, en (4), en la ecuación corresopondiente a la σ_j que es el automorfismo identidad, tendríamos

$$\omega_1 a_1 + \cdots + \omega_r = 0$$

contradiciendo la independencia lineal de $\omega_1, \ldots, \omega_{n+1}$. Otra vez podemos asumir que $a_i \notin \mathbb{E}^G$, pues si no es así, bastará un nuevo reordenamiento de la base.

Esto significa que existe $\sigma_k \in G$ tal que $\sigma_k(a_1) \neq a_1$, pues a_1 no pertenece al campo fijado por G. Analizando la j-esima ecuación de (4)

$$\sigma_j(\omega_1)a_1 + \cdots + \sigma_k j\omega_r) = 0$$

y al aplicarle σ_k, obtenemos

$$\sigma_k\sigma_j(\omega_1)\sigma_k(a_1) + \cdots + \sigma_k\sigma_j(\omega_r) = 0. \tag{5}$$

Como G es un grupo, $\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots, \sigma_k\sigma_n$ es una permutación de $\sigma_1, \sigma_2, \ldots, \sigma_n$. Haciendo $\sigma_k\sigma_j = \sigma_i$, la i-ésima ecuación de (5) es

$$\sigma_i(\omega_1)\sigma_k(a_1) + \cdots + \sigma_i(\omega_r) = 0.$$

Restando esta i-ésima ecuación de la i-ésima ecuación original obtenemos:

$$\begin{gathered}\sigma_i(\omega_1)a_1 + \cdots + \sigma_i(\omega_r) - \sigma_i(\omega_1)\sigma_k(a_1) + \cdots + \sigma_i(\omega_r) = \\ \sigma_i(\omega_1)[a_1 - \sigma_k(a_1)] + \cdots + \sigma_i(\omega_1)[a_{r-1} - \sigma_k(a_{r-1})] + \sigma_i(\omega_r) - \sigma_i(\omega_r) = \\ \sigma_i(\omega_1)[a_1 - \sigma_k(a_1)] + \cdots + \sigma_i(\omega_1)[a_{r-1} - \sigma_k(a_{r-1})].\end{gathered}$$

Como $a_1 - \sigma_k(a_1) \neq$, hemos encontrado una solución no trivial para (4) con menos de r componentes no 0. Lo cual es una contradicción.

Hilbert

Definición 8 *Sea E/F una extensión de Galois y sea $\alpha \in E\backslash\{0\}$. Definimos la norma $N(\alpha)$ de α por*

$$N(\alpha) := \prod_{\sigma \in Gal(E/F)} \sigma(\alpha).$$

Teorema 9 (Teorema de Hilbert) *Sea E/F una extensión de Galois cuyo grupo de Galois $G = Gal(E/F)$ es cíclico de orden n. Sea σ un generador de G. Entonces $N(\alpha) = 1$ si y sólo si existe $\beta \in E \setminus \{0\}$ tal que*

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

Demostración: Si $\alpha = \beta\sigma(\beta)^{-1}$, entonces

$$\begin{aligned} N(\alpha) &= N(\beta\sigma(\beta)^{-1}) \\ &= N(\beta)N\big(\sigma(\beta)^{-1}\big) \\ &= N(\beta)N\big(\sigma(\beta)\big)^{-1} \\ &= N(\beta)N(\beta)^{-1} \\ &= 1. \end{aligned}$$

Para probar la implicación contraria definamos la siguiente sucesión

$$\begin{aligned} \delta_0 &= \alpha, \\ \delta_1 &= \alpha\sigma(\alpha), \\ \delta_2 &= \alpha\sigma(\alpha)\sigma^2(\alpha), \\ &\vdots \\ \delta_{n-1} &= \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha). \end{aligned}$$

Dado que $\langle\sigma\rangle = Gal(E/F)$, tenemos que $\delta_{n-1} = N(\alpha) = 1$. Ahora, tenemos que para toda $i \in \{0, 1, \ldots, n-2\}$ se tiene que

$$\alpha\sigma(\delta_i) = \delta_{i+1}. \tag{6}$$

Tenemos que los caracteres $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ son independientes, por lo tanto existe $\gamma \in E$ tal que

$$\delta_0\gamma + \delta_1\sigma(\gamma) + \delta_2\sigma^2(\gamma) + \cdots + \delta_{n-2}\sigma^{n-2}(\gamma) + \sigma^{n-1}(\gamma) = \beta \neq 0.$$

Usando la ecuación (6) se tiene que

$$\sigma(\beta) = \alpha^{-1}\big[\delta_1\sigma(\gamma) + \delta_2\sigma^2(\gamma) + \cdots + \delta_{n-1}\sigma_{n-1}(\gamma)\big] + \sigma^n(\gamma).$$

Como $\sigma^n = 1$, se tiene que el último sumando es $\gamma = \alpha^{-1}\delta_0\gamma$. Factorizando α^{-1} tenemos que $\sigma(\beta) = \alpha^{-1}\beta$, por lo tanto $\alpha = \beta\sigma(\beta)^{-1}$.

Hall

Teorema 10 (Hall) *Sea G un grupo finito soluble de orden mn, donde m y n son primos relativos. Entonces existe un subgrupo $H \leq G$ de orden n.*

Demostración: Sea π el conjunto de los primos que dividen a n. Sea M un subgrupo de G normal minimal. Tenemos que existe un primo p tal que M es un p-grupo elemental abeliano. Dividiremos en dos casos.

Caso 1. Supongamos que $p \in \pi$. Sea $|M| = p^\alpha$. Entonces

$$|G/M| = \frac{mn}{p^\alpha} = mn_1,$$

donde $n = n_1 p^\alpha$. Por inducción el resultado se cumple para G/M. El Teorema de la Correspondencia nos dice que un π-subgrupo de Hall de G/M es de la forma H/M, donde H es un subgrupo de G que contiene a M. Entonces $|H/M| = n_1$, por lo tanto

$$|H| = n_1|M| = n_1 p^\alpha = n.$$

Caso 2. No hay grupos normales minimales de G que sean p-subgrupos elementales abelianos para $p \in \pi$. En particular nuestro subgrupo normal minimal M satisface $|M| = q^\beta$, con $q \notin \pi$. Entonces

$$|G/M| = \frac{mn}{q^\beta} = m_1 n,$$

donde $m = m_1 q^\beta$. Ahora subdividiremos en dos casos de acuerdo a n_1.

Subcaso 2.1 Supongamos que $m_1 \neq 1$. Entonces, por inducción tenemos que G/M tiene un π-subgrupo de Hall, el cual tiene la forma K/M, donde K es un subgrupo de G que contiene a M y

$$|K/M| = n.$$

Entonces

$$|K| = n|M| = nq^\beta = \frac{mn}{m_1} < mn.$$

Aplicaremos nuevamente inducción a K, el cual tiene un orden más pequeño que el de G y, por lo tanto, tiene un π-subgrupo de Hall H. Entonces $|H| = n$, así que H también es un subgrupo de Hall de G.

Subcaso 2.2 Supongamos que $m_1 = 1$, entonces $|G| = nq^\beta$. Tenemos que $|G/M| = m > 1$. Sea N/M un subgrupo normal minimal de G/M. Entonce existe un primo $p \in \pi$ tal que N/M es un p-grupo elemental abeliano. Sea α tal que $|N/M| = p^\alpha$. Entonces $N \trianglelefteq G$ y

$$|N| = p^\alpha q^\beta.$$

Sea P un p-subgrupo de Sylow de N. Entonces aplicando el Argumento de Frattini tenemos que

$$G = N_G(P)N.$$

Y como $N = PM$, tenemos que

$$G = N_G(P)PM = N_G(P)M.$$

Ahora consideremos $J = N_G(P) \cap M$. Dado que M es abeliano, tenemos que $J \trianglelefteq M$, y también $J = N_G(P) \cap M \trianglelefteq N_G(P)$, dado que $M \trianglelefteq G$. Por lo tanto

$$J \trianglelefteq N_G(P)M = G.$$

Pero M es un subgrupo normal minimal de G, así que $J = 1$ o $J = M$.

Si $J = N_G(P) \cap M = M$, entonces $M \leq N_G(P)$, así que $G = N_G(P)$. Por lo tanto P es un p-subgrupo normal de G y algún subgrupo de P es un subgrupo normal minimal de G, y entonces es un p-subgrupo elemental abeliano con $p \in \pi$. Esto contradice la suposición general para el *Caso 2.*

Entonces $J = 1$, y así $N_G(P) \cap M = 1$. Ahora

$$nq^\beta = |G| = |N_G(P)M| = |N_G(P)| \cdot |M|,$$

así que $|N_G(P)| = M$. Por lo tanto $H = N_G(P)$ es el π-subgrupo de Hall que buscabamos.

An es simple

Lema 5 *Para toda $n \in \mathbb{N}$, si $n \geq 3$, entonces todo elemento de A_n es producto de 3-ciclos.*

Demostración: Sea $\alpha \in A_n$. Entonces existe una cantidad par de transposiciones $\tau_1, \tau_2, \ldots, \tau_{2q} \in S_n$ tales que

$$\alpha = \tau_1 \tau_2 \cdots \tau_{2q}.$$

Sin pérdida de generalidad podemos asumir que para toda $i \in \{1, 2, \ldots, q\}$ se tiene que $\tau_{2i-1} \neq \tau_{2i}$. Entonces tenemos dos casos.

Caso 1. Si $\tau_{2i} - 1$ y τ_{2i} no son transposiciones disjuntas tenemos que

$$\begin{aligned} \tau_{2i} - 1\tau_{2i} &= (i\ j)(j\ k) \\ &= (i\ j\ k). \end{aligned}$$

Caso 2. Si $\tau_{2i} - 1$ y τ_{2i} son transposiciones disjuntas tenemos que

$$\begin{aligned} \tau_{2i} - 1\tau_{2i} &= (i\ j)(k\ l) \\ &= (i\ j)(j\ k)(j\ k)(k\ l) \\ &= (i\ j\ k)(j\ k\ l). \end{aligned}$$

Teorema 11 *Para toda $n \in \mathbb{N}$, si $n \geq 5$, entonces A_n es un grupo simple.*

Demostración: Primero probaremos que A_5 es un grupo simple. Sea $Id_5 \lneq H \trianglelefteq A_5$. Sea $Id_5 \neq \sigma \in H$. Sin pérdida de generalidad podemos asumir que $\sigma = (1\ 2\ 3)$, $\sigma = (1\ 2)(3\ 4)$ o $\sigma = (1\ 2\ 3\ 4\ 5)$. Si σ es un 3-ciclo tenemos que, como todos los 3-ciclos son conjugados en A_n, entonces todos los 3-ciclos están en H y, por el lema anterior tenemos que $H = A_5$. Si $\sigma = (1\ 2)(3\ 4)$, definimos $\tau = (1\ 2)(3\ 5)$. Tenemos que H contiene a $(\tau\sigma\tau^{-1})\sigma^{-1} = (3\ 4\ 5)$, dado que H es un subgrupo normal, con lo que concluímos que $H = A_5$. Si $\sigma = (1\ 2\ 3\ 4\ 5)$, definimos $\rho = (1\ 3\ 2)$. Tenemos que H contiene a $(\rho\sigma\rho^{-1})\sigma^{-1} = (1\ 3\ 4)$, dado que H es un subgrupo normal, con lo que concluímos de igual forma que $H = A_5$.

Para probar que A_6 es un grupo simple tomemos $Id_5 \lneq H \trianglelefteq A_6$. Supongamos primero que existe un elemento $\alpha \in H$ y existe $i \in \{1, 2, \ldots, 6\}$ tales que $\alpha(i) = i$. Sea

$$F = \{\sigma \in A_6 : \sigma(i) = i\}.$$

Notemos que $\alpha \in H \cap F$, por lo tanto $H \cap F \neq \{Id_5\}$. El Segundo Teorema de Isomorfismo nos dice que $H \cap F \lhd F$. Como $F \cong A_5$, tenemos que es simple y por lo tanto $H \cap F = F$, lo que es decir que $F \leq H$. De aquí tenemos que H contiene un 3-ciclo y, por lo tanto, $H = A_6$. Ahora supongamos que no existe en H tal elemento α no trivial que fije a alguna i. Tenemos que α sólo puede tener la estructura cíclica $(1\ 2)(3\ 4\ 5\ 6)$ o $(1\ 2\ 3)(4\ 5\ 6)$. En el primer caso tenemos que el cuadrado de la permutación fija a un punto, por lo tanto no puede tener dicha estructura. En el segundo caso tenemos que la permutación $\alpha(\beta\alpha^{-1}\beta^{-1})$, donde $\beta = (2\ 3\ 4)$, y se puede verificar facilmente que éste es un elemento no trivial que fija a un punto, por lo tanto α tampoco puede tener dicha estructura cíclica, con lo que concluímos que un grupo H así no puede existir.

Por último probaremos que para $n \geq 7$ tenemos que A_n es simple. Sea $Id_5 \lneq H \trianglelefteq A_n$. Sea $\beta \in H$ un elemento no trivial y sea i un punto movido por β. Sea α un 3-ciclo que mueva a $j = \beta(i)$ y que fije a i. Es fácil ver que $\beta\alpha \neq \alpha\beta$. De aquí se sigue que el elemento $\gamma = \alpha(\beta\alpha^{-1}\beta^{-1})$ es no trivial. Tenemos que $\beta\alpha^{-1}\beta^{-1}$ es un 3-ciclo, por lo tanto γ es un producto de dos 3-ciclos, de donde tenemos que γ mueve a, a lo más, 6 puntos. Si aplicamos la misma técnica que en el párrafo anterior tenemos el resultado completo.

Dedekind-Baer

Definición 12 *Un grupo no abeliano G es* ***Hamiltoniano*** *si todos sus subgrupos son normales.*

Antes de pasar a la demostración del teorema de Dedekind-Baer, necesitaremos el siguiente lema.

Lema 6 *Sea G un grupo y $x, y \in G$ tales que $[x, y]$ conmuta con x y y. Entonces*

(i) $[x^i, y^j] = [x, y]^{ij}$, *donde* $i, j \in \mathbb{Z}$.

(ii) $(xy)^i = x^i y^i [y, x]^{\binom{i}{2}}$, *donde* $i \in \mathbb{N}$.

Teorema 13 (Dedekind, Baer) *G es Hamiltoniano si y sólo si*

$$G \cong Q_8 \times A \times B$$

donde Q_8 es el grupo de los cuaterniones, A es un 2-grupo abeliano elemental, y B es un gruop abeliano donde sus elementos son de orden impar.

Demostración: Suficiencia. Sea $H < G$. Entonces $H = (H \cap (Q_8 \times A)) \times (H \cap B)$. Es suficiente mostrar que $H_1 = H \cap (Q_8 \times A) \triangleleft Q_8 \times A$. Si H_1 contiene un elemento de orden 4 (quien forzosamente pertenece a Q_8), entonces $\{h^2 : h \in H_i\} = Z(Q_8) = G' =\subset H_1$, así que $H \triangleleft G$. Si H_1 no contiene a un elemento de orden 4, (no contiene a alguno de los generadores de Q_8), entonces $H_1 \subset Z(G)$ y $H_1 \triangleleft G$.

Necesidad. Sean $x, y \in G$ tales que $c = [x, y] \neq 1$. Como $< x >, < y > \triangleleft G \Leftrightarrow c \in < x > \cap < y >$. Es decir, para algunos $i, j \in \mathbb{Z}$ tenemos $c = x^i = y^j$. Si definimos $Q =< x, y >$, entonces $Q' =< c >\subset Z(Q)$. Por el lema 6, $c^i = [x^i, y] = [c, y] = 1$ y por lo tanto x, y son de orden finito.

Supóngase ahora que $o(x) + o(y)$ es mínimo (donde o denota "orden de"). Sea p un factor primo de $o(x)$. La minimalidad de $o(x) + o(y)$ implica que $1 = [x^p, y] = c^p$. Así que $o(c) = p$. También, $o(x)$ no puede tener factores primos distintos de p, así que $o(x)$ (y $o(y)$) tienen que ser potencias de p. Escribamos ahora $c = x^{\alpha p^r} = y^{\beta p^s}$ con $\alpha, \beta \in Z$ y $r, s \in \mathbb{N}$ tales que $p \nmid \alpha, \beta$. Entonces $o(x) = p^{r+1}$ y $o(s) = p^{s+1}$. Sean ahora $\alpha', \beta' \in \mathbb{Z}$ tales que $\alpha'\alpha \equiv \beta'\beta \equiv 1 \,(mod\, p)$. Entonces

$$x^{\beta' p^r} = x^{\beta'\alpha'\alpha p^r} = c^{\alpha'\beta'} = y^{\alpha'\beta'\beta p^s} = y^{\alpha' p^s}$$

de donde $c^{\alpha'\beta'} = [x^{\beta'}, y^{\alpha'}]$. Remplazando x, y, c por $x^{\beta'}, y^{\alpha'}, c^{\alpha'\beta'}$ respectivamente. Dicho todo esto, podemos suponer que $x^{p^r} = y^{p^s} = c$. Nótese que $r, s > 0$ o de otra manera ocurriría que $[x, y] = 1$.

Sin pérdida de generalidad, supongamos que $r \geq s$. Como $x^{-p^{r-s}}y$ no conmuta con x, por la minimalidad de $o(x)+o(y)$, $o(x^{-p^{r-s}}y) \geq o(y) = p^{s+1}$. Por la segunda parte de 6,

$$1 \neq (x^{-p^{r-s}}y)^{p^s} = x^{-p^r}y^{-p^s}[y, x^{-p^{r-s}}]^{\binom{p^s}{2}} = [y,x]^{-p^{r-s}\binom{p^s}{2}} = c^{-\frac{1}{2}p^r(p^s-1)}.$$

Así que, $p \nmid \frac{1}{2}p^r(p^s-1)$ y por lo tanto, p está forzado a ser 2 y entonces r a ser 1. Entonces $o(x) = 4$, $x^2 = y^2$, $yxy^{-1} = x^{-1}$ y estas condiciones, junto que Q es no abeliano, forzan a Q a ser isomorfo a Q_8.

Veamos que $G = QC$, donde $C = C_G(Q)$. Sea $g \in G$, Entonces $gxg^{-1} = x^{\pm 1} = x^{(-1)^a}$ y análogamente para y, $gyg^{-1} = y^{\pm 1} = y^{(-1)^b}$, con $a, b \in \{0,1\}$. Es decir que $y^a x^b g$ conmuta con x y x y por lo tanto $y^a x^b g \in C$.

Veamos ahora que C no contiene elementos de orden 4. Supongamos lo contrario y sea $g \in C$ de orden 4. Por ser de orden 4 y pertencer a C, g no puede estar en Q. Así que $o(gx) = 2$ ó 4. Como $[gx, y] \neq 1$, $ygxy^{-1} = (gx)^1$, es decir, que $g = g^{-1}$, contradiciendo que g tenía orden 4.

Ahora, tenemos que C es abeliano. De lo contrario C sería un grupo Hamiltoniano sin elementos de orden 4. Contradiciendo que Q es isomorfo a Q_8.

Veamos ahora que para cada $g \in G$, gx no conmuta con y. Tenemos que $o(gx) < \infty$ y por lo tanto $o(g) < \infty$. Entonces, C tiene que ser periódico (de torsión). Y por lo tanto, después de todo lo dicho anteriormente, debe ser de la forma $C = A \times B$, con A un 2-grupo elemental abeliano y con B un grupo donde todos sus elementos son de orden impar. Y con esto, termina la demostración.