Producto semidirecto de grupos

Sésar

1. Definición y ejemplos

Sabemos que dado un grupo G y un conjunto arbitrario $X \neq \varnothing$, entonces G actúa sobre X si $\exists \varphi : G \to S(X)$ homomorfismo, donde $S(x)$ es el grupo de permutaciones en X. Nuestra atención se pondrá en el caso concreto donde $X = N \trianglelefteq G$ y considerando el grupo de automorfismos $\mathrm{Aut}(N)$ —es decir, el grupo de los endomorfismos en N biyectivos—.

Definition 1. Sean H y N grupos. Diremos que H **actúa vía automorfismos** sobre N si existe un $\phi : H \to \mathrm{Aut}(N)$ homomorfismo.

Para simplifcar la notación, escribiremos $\phi_h(n) := \phi(h)(n)$ para todo $n \in N$ y $h \in H$.

Example 1. Estos son algunos ejemplos inmediatos de grupos actuando vía automorfismos sobre otros.

1. Si $H \leq \mathrm{Aut}(N)$, entonces la aplicación inmersión $\imath : H \hookrightarrow \mathrm{Aut}(N)$ es una acción vía automorfismos llamada la **acción natural**.

2. Toda acción por conjugación es una acción vía automorfismos: si $N \trianglelefteq G$ y $H \leq G$, entonces

$$\begin{aligned} \phi : H &\to \mathrm{Aut}(N) \\ h &\mapsto \phi_h(n) := hnh^{-1}. \end{aligned}$$

   Además, $\ker \phi = \{h \in H \mid \phi_h(n) = n,\ \forall n \in N\} = \{h \in H \mid hn = nh,\ \forall n \in N\} = C_H(N)$.

3. La **acción trivial** $\phi : H \to \mathrm{Aut}(N)$ tal que $\phi_h := \mathrm{id}_N$ es una acción vía automorfismos.

Theorem 1. Supongamos que $\phi : H \to \mathrm{Aut}(N)$ es una acción vía automorfismos. Definamos la siguiente operación en $N \times H$:

$$(n_1, h_1) *_\phi (n_2, h_2) := (n_1 \phi_{h_1}(n_2), h_1 h_2).$$

Entonces $(N \times H, *_\phi)$ es un grupo.

Demostración. En primer lugar, es fácil comprobar que la operación está bien definida ya que $h_1 h_2 \in H$ —por ser H un grupo— y por definición de ϕ, $\phi_{h_1}(n_2) \in N$ y como N es otro grupo, $n_1 \phi_{h_1}(n_2) \in N$. De este modo, basta comprobar que $*_\pi$ es asociativa, y existe un elemento netruo y elementos inversos en la operación.

Asociatividad: En primer lugar, calculamos lo siguiente:

$$[(n_1,h_1) *_\phi (n_2,h_2)] *_\phi (n_3,h_3) = (n_1\phi_{h_1}(n_2), h_1h_2) *_\phi (n_3,h_3) = (n_1\phi_{h_1}(n_2)\phi_{h_1h_2}(n_3), h_1h_2h_3).$$

Por el otro lado, calculamos lo siguiente:

$$(n_1,h_1) *_\phi [(n_2,h_2) *_\phi (n_3,h_3)] = (n_1,h_1) *_\phi (n_2\phi_{h_2}(n_3), h_2h_3) = (n_1\phi_{h_1}(n_2\phi_{h_2}(n_3)), h_1h_2h_3).$$

No obstante, como $\phi_{h_1} \in \mathrm{Aut}(N)$, entonces $\phi_{h_1}(n_2\phi_{h_2}(n_3)) = \phi_{h_1}(n_2)\phi_{h_1}(\phi_{h_2}(n_3))$ y como ϕ es un homomorfismo, entonces $\phi_{h_1}(\phi_{h_2}(n_3)) = \phi_{h_1h_2}(n_3)$, dándose la igualdad deseada.

Elemento neutro: Demostremos que (e_N, e_H) es el elemento neutro para esta operación.

$$\begin{aligned}(n,h) *_\phi (e_N,e_H) &= (n\phi_h(e_N), he_H) = (n,h),\\ (e_N,e_H) *_\phi (n,h) &= (e_N\phi_{e_H}(n), e_Hh) = (n,h).\end{aligned}$$

Elemento inverso: Demostremos que para todo $(n,h) \in N \times H$, $(n,h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$.

$$\begin{aligned}(n,h) *_\phi (\phi_{h^{-1}}(n^{-1}), h^{-1}) &= (n\phi_h(\phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n\phi_{hh^{-1}}(n^{-1}), e_H) = (e_N, e_H),\\ (\phi_{h^{-1}}(n^{-1}), h^{-1}) *_\phi (n,h) &= (\phi_{h^{-1}}(n^{-1})\phi_{h^{-1}}(n), h^{-1}h) = (e_N, e_H).\end{aligned}$$

□

Definition 2. Sean H y N grupos y $\phi : H \to \mathrm{Aut}(N)$ una acción vía automorfismos. El **ϕ-producto semidirecto** de H y N es el grupo

$$N \rtimes_\phi H := (N \times H, *_\phi).$$

Si la acción vía automorfismos es claro por el contexto, entonces puede omitirse de la notación como $N \rtimes H$.

Remark 1. Si N y H son finitos, entonces $|N \rtimes_\phi H| = |N||H|$.

Example 2. Veamos algunos ejemplos sencillos de productos semidirectos

1. Si ϕ es la acción trivial, entonces $N \rtimes_\phi H = N \times H$, es decir, el producto directo.
2. Llamamos grupo **holomorfo** al grupo $\mathrm{Hol}(N) := N \rtimes_\phi \mathrm{Aut}(N)$, donde ϕ es la acción natural de $H = \mathrm{Aut}(N)$ sobre N.

Theorem 2. Sea $\phi : H \to \mathrm{Aut}(N)$ acción vía automorfismos y $G = N \rtimes_\phi H$. Sea $\widetilde{N} := N \times \{e_H\}$ y $\widetilde{H} := \{e_N\} \times H$.

1. $\widetilde{H}, \widetilde{N} \leq G$.
2. $\widetilde{N} \trianglelefteq G$.
3. $\widetilde{N} \cong N$ y $\widetilde{H} \cong H$.

Demostración. Probaremos cada punto por separado.

1. Empecemos comprobando que $\widetilde{H}$ es un subgrupo. Claramente, $(e_N, e_H) \in \widetilde{H}$. Por otro lado, si $(e_N, h_1), (e_N, h_2) \in \widetilde{H}$, entonces

$$(e_N, h_1) *_\phi (e_N, h_2) = (e_N\phi_{h_1}(e_N), h_1h_2) = (e_N, h_1h_2) \in \widetilde{H}.$$

Finalmente, $(e_N, h)^{-1} = (\phi_{h^{-1}}(e_N^{-1}), h^{-1}) = (e_N, h^{-1}) \in \widetilde{H}$.

Veamoslo ahora para $\widetilde{N}$. También tenemos $(e_N, e_H) \in \widetilde{H}$. Ahora, si $(n_1, e_H), (n_2, e_H) \in \widetilde{N}$, entonces

$$(n_1, e_H) *_\phi (n_2, e_H) = (n_1 \phi_{e_H}(n_2), e_H e_H) = (n_1 n_2, e_H) \in \widetilde{N}.$$

Por último, $(n, e_H)^{-1} = (\phi_{e_H}(n^{-1}), e_H^{-1}) = (n^{-1}, e_H) \in \widetilde{N}$.

2. Basta demostrar que para todo $(n', e_H) \in \widetilde{N}$ y $(n, h) \in G$, $(n, h) *_\phi (n', e_H) *_\phi (n, h)^{-1} \in \widetilde{N}$.

$$\begin{aligned}(n, h) *_\phi (n', e_H) *_\phi (n, h)^{-1} &= (n\phi_h(n'), h) *_\phi (\phi_{h^{-1}}(n^{-1}), h^{-1}) = \\ &= (n\phi_h(n')\phi_h(\phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n\phi_h(n')n^{-1}, e_H) \in \widetilde{N},\end{aligned}$$

puesto que $\phi_h(n') \in N$ y por tanto $n\phi_h(n')n^{-1} \in N$.

3. Es fácil comprobar por el punto 1 de esta demostración que las aplicaciones

$$\begin{array}{ccc} H \to \widetilde{H} & y & N \to \widetilde{N} \\ h \mapsto (e_N, h) & & n \mapsto (n, e_H) \end{array}$$

son isomorfismos. □

Corollary 1. Sea $G = N \rtimes_\phi H$. Las siguientes afirmaciones son equivalentes.

1. $G = N \times H$.
2. $\widetilde{H} \trianglelefteq G$.
3. $\phi_h = \mathrm{id}_N$ para todo $h \in H$.

Demostración. Probaremos las equivalencias en el orden presentado por el corolario.

$(1 \Rightarrow 2)$ Como G es un producto directo, en particular $\widetilde{H} \trianglelefteq G$.

$(2 \Rightarrow 3)$ Tomemos $h \in H$ y $n \in N$. Entonces

$$(n, e_H)^{-1} *_\phi (e_N, h) *_\phi (n, e_H) = (n^{-1}, e_H) *_\phi (n, h) = (n^{-1}\phi_h(n), h).$$

Como $\widetilde{H} \trianglelefteq G$, entonces $(n^{-1}\phi_h(n), h) \in \widetilde{H}$, lo que implica que $n^{-1}\phi_h(n) = e_N$, es decir, $\phi_h(n) = n$. Como esto es cierto para todo $n \in N$, entonces $\phi_h = \mathrm{id}_N$ para todo $h \in H$.

$(3 \Rightarrow 1)$ En este caso, la operación que se define es la siguiente:

$$(n_1, h_1) *_\phi (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2) = (n_1n_2, h_1h_2),$$

que es la operación del producto directo. Luego $G = N \times H$.

□

Theorem 3 (de Isomorfía del producto semidirecto)**.** Supongamos que $H \overset{\alpha}{\cong} \widehat{H}$ y $N \overset{\beta}{\cong} \widehat{N}$. Sea $\phi : H \to \mathrm{Aut}(N)$ acción vía automorfismos.

1. $\widehat{\beta} : \mathrm{Aut}(N) \to \mathrm{Aut}(\widehat{N})$ tal que $\widehat{\beta}(f) := \beta \circ f \circ \beta^{-1}$ es un isomorfismo.

2. $\widehat{\phi} : \widehat{H} \to \operatorname{Aut}(\widehat{N})$ definido como $\widehat{\phi} := \widehat{\beta} \circ \phi \circ \alpha^{-1}$ es una acción vía automorfismos.
3. $N \rtimes_\phi H \cong \widehat{N} \rtimes_{\widehat{\phi}} \widehat{N}$.

$$\begin{tikzcd}
H \arrow[r, "\phi"] \arrow[d, "\alpha"'] & \operatorname{Aut}(N) \arrow[d, "\widehat{\beta}"] \\
\widehat{H} \arrow[r, "\widehat{\phi}"'] & \operatorname{Aut}(\widehat{N})
\end{tikzcd}$$

Demostración. Demostraremos cada apartado en el orden establecido.

1. Es claro observar que $\widehat{\beta}$ es la acción por conjugación sobre $\widehat{N}$, luego es un homomorfismo. Además, la biyección es clara de comprobar.
2. Como $\widehat{\phi}$ está definida como la composición de homomorfismos —notemos que α es un isomorfismo por hipótesis—, entonces es también un homomorfismo.
3. Definamos la siguiente aplicación:

$$\begin{aligned} f : N \rtimes_\phi H &\to \widehat{N} \rtimes_{\widehat{\phi}} \widehat{N} \\ (n, h) &\mapsto (\beta(n), \alpha(h)). \end{aligned}$$

Por la biyección de α y β, podemos concluir que f es también biyectiva. Falta mostrat que f es un homomorfismo de grupos. En primer lugar tenemos lo siguiente:

$$\begin{aligned} f((n_1, h_2) *_\phi (n_2, h_2)) &= f(n_1 \phi_{h_1}(n_2), h_1 h_2) = (\beta(n_1 \phi_{h_1}(n_2)), \alpha(h_1 h_2)) = \\ &= (\beta(n_1)\beta(\phi_{h_1}(n_2)), \alpha(h_1)\alpha(h_2)). \end{aligned}$$

Por otro lado, fijémonos que

$$\widehat{\phi}_{\alpha(h)}(\beta(n)) = (\widehat{\beta} \circ \phi \circ \alpha^{-1})_{\alpha(h)}(\beta(n)) = (\widehat{\beta} \circ \phi_h)(\beta(n)) = \beta(\phi_h(n)).$$

De este modo, obtenemos que

$$\begin{aligned} f(n_1, h_1) *_{\widehat{\phi}} f(n_2, h_2) &= (\beta(n_1), \alpha(h_1)) *_{\widehat{\phi}} (\beta(n_2), \alpha(h_2)) = \\ &= (\beta(n_1)\widehat{\phi}_{\alpha(h_1)}(\beta(n_2)), \alpha(h_1)\alpha(h_2)) = \\ &= (\beta(n_1)\beta(\phi_{h_1}(n_2)), \alpha(h_1)\alpha(h_2)). \end{aligned}$$

Se concluye de esta manera que f es un isomorfismo. □

Corollary 2. Sea $\phi : H \to \operatorname{Aut}(N)$ acción vía automorfismos y $\varphi : \widetilde{N} \rtimes_\phi H \to \operatorname{Aut}(N)$ la acción por conjugación. Entonces

$$N \rtimes_\phi H \cong \widetilde{N} \rtimes_{\varphi|_{\widetilde{H}}} \widetilde{H}.$$

Demostración. Por un lado, sabemos que $\alpha : H \to \widetilde{H}$ donde $\alpha(h) = (e_N, h)$ es un isomorfismo. Además, como $\beta : N \to \widehat{N}$ es también un isomorfismo, entonces $\widetilde{\beta} : \mathrm{Aut}(N) \to \mathrm{Aut}(\widetilde{N})$ donde $\widetilde{\beta}(f) = \beta \circ f \circ \beta^{-1}$ —es decir, $\widetilde{\beta}(f)(n, e_H) = (f(n), e_H)$— es un isomorfismo. Si demostramos que la acción por conjugación $\varphi|_{\widetilde{H}} = \widetilde{\beta} \circ \phi \circ \alpha^{-1}$, entonces por el Teorema de Isomorfía del producto semidirecto se tiene lo deseado.

Por un lado, tenemos que para todo $h \in H$,

$$\varphi|_{\widetilde{H}}(\alpha(h)) = \varphi(e_N, h) \in \mathrm{Aut}(\widetilde{N}).$$

Tomando $(n, e_H) \in \widetilde{N}$ arbitrario,

$$\varphi(e_N, h)(n, e_N) = (n, e_H) *_\phi (e_N, h) *_\phi (n, e_H)^{-1} = (e_N \phi_h(n) e_N^{-1}, e_H) = (\phi_h(n), e_H).$$

Por definición de β, tenemos que $(\phi_h(n), e_H) = \widetilde{\beta}(\phi_h)(n, e_H)$. En resumen, tenemos que para todo $n \in N$, $\varphi(e_N, h)(n, e_N) = \widetilde{\beta}(\phi_h)(n, e_H)$, luego obtenemos que $\varphi|_{\widetilde{H}}(\alpha(h)) = \widetilde{\beta}(\phi(h))$. Como esto es cierto para todo $h \in H$, entonces se tiene lo deseado. □

2. Extensión de grupos

Definition 3. Sea G un grupo, $H \leq G$ y $N \trianglelefteq G$. Decimos que G es una **extensión** de N sobre H si

1. $G = NH$,
2. $N \cap H = \{e\}$.

También decimos en el contexto de la definición anterior que G **se escinde** sobre N y al subgrupo H lo llamamos **complemento** de H.

Theorem 4. Sea G un grupo, $H \leq G$ y $N \trianglelefteq G$. Son equivalentes:

1. G es una extensión de N sobre H.
2. $\forall g \in G$, $\exists! h \in H$ y $n \in N$ tal que $g = nh$.
3. $\forall g \in G$, $\exists! h \in H$ y $n \in N$ tal que $g = hn$.
4. Si $\imath : H \hookrightarrow G$ y $\pi : G \to G/N$, entonces $\pi \circ \imath$ es un isomorfismo.
5. $\exists f : G \to H$ homomorfismo tal que $f|_H = \mathrm{id}_H$ y $\ker f = N$.

Demostración. Probaremos las equivalencias en el orden presentado por el teorema.

(1⇒2) Supongamos que $g = n_1 h1 = n_2 h_2$. Entonces $n_2^{-1} n_1 h_1 h_2^{-1} = e \in N \cap H$. Por un lado, $n_2^{-1} n_1 \in N$ y como $h_2 h_1^{-1} \in H$, entonces $n_2^{-1} n_1 = (n_2^{-1} n_1 h_1 h_2^{-1})(h_2 h_1^{-1}) \in H$. Por tanto, $n_2^{-1} n_1 \in N \cap H = \{e\}$, luego $n_1 = n_2$. Por tanto, $e = n_2^{-1} n_1 h_1 h_2^{-1} = h_1 h_2^{-1}$ por lo que se demuestra además que $h_1 = h_2$.

(2⇒3) Sea $g = nh$, entonces $g = h(h^{-1} n h) \in HN$ ya que N es un subgrupo normal. Supongamos ahora que $g = h' n'$. Entonces $g = (h' n' (h')^{-1}) h' \in NH$. Por la hipótesis de la escritura única de g, tenemos que $h = h'$ y por tanto, $h n' h^{-1} = n$, por lo que $n' = h^{-1} n h$, por lo que la escritua en este orden es también única.

(3⇒4) Sabemos que la composición de homomorfismos es un homomorfismo. Falta demostrar la biyección de esta aplicación.

Sea $h \in \ker(\pi \circ \imath)$, entonces $\pi \circ \imath(h) = \pi(h) = hN = eN$. Esto implica que $h \in N$. De este modo, nos encontramos con que h puede expresarse de dos maneras como producto de un elemento de H y de N. En primer lugar, $h = he$ donde $h \in H$ y $e \in N$ y por otro lado $h = eh$, donde $e \in H$ y $h \in N$ por el comentario anterior. Como por hipótesis esta representación es única, tenemos que $h = e$, luego $\ker(\pi \circ \imath) = \{0\}$ y la aplicación es inyectiva.

Tomemos ahora $gN \in G/N$. Por hipótesis, $g = hn$ donde $h \in H$ y $n \in N$ son únicos. Por tanto, $\pi(\imath(h)) = hN = (hn)N = gN$, demostrando así la propiedad sobreyectiva de la aplicación.

(4⇒5) Por hipótesis, $\pi \circ \imath : H \to G/N$ es un isomorfismo. Tomemos la aplicación $f = (\pi \circ \imath)^{-1} \circ \pi : G \to H$. Esta aplicación f es homomorfismo por ser composición de homomorfismos. Además, $f|_H = f \circ \imath = (\pi \circ \imath)^{-1} \circ \pi \circ \imath = \mathrm{id}_H$. Finalmente, $\ker f = \ker \pi = N$.

(5⇒1) Sea $g \in G$. Entonces $f(g) \in H$ por hipótesis. Por otro lado, $gf(g^{-1}) \in \ker f$ ya que $f(gf(g^{-1})) = f(g)f(f(g^{-1})) = f(g)f(g^{-1}) = e$, esto debido a que $f|_H = \mathrm{id}_H$. Así pues, $gf(g^{-1}) \in N$. Como $g = gf(g^{-1})f(g)$, entonces $g \in NH$. Por otro lado, supongamos que $g \in N \cap H$. Por un lado, como $g \in H$, entonces $g = f(g)$. Por otro lado, $g \in N$, luego $f(g) = e$, por lo que $g = e$ y $N \cap H = \{e\}$. □

Theorem 5 (Condición suficiente de la extensión)**.** Sea $\phi_H \to \mathrm{Aut}(N)$ una acción vía automorfismos. Entonces $N \rtimes_\phi H$ es una extensión de $\widetilde{N}$ sobre $\widetilde{H}$.

Demostración. En primer lugar, vemos que para todo $(n,h) \in N \times H$, tenemos que

$$(n, e_H) *_\phi (e_N, h) = (n\phi_{e_H}(e_N), h) = (n, h),$$

luego $N \rtimes_\phi H = \widetilde{N} *_\phi \widetilde{H}$. Por otro lado, es fácil comprobar que $\widetilde{N} \cap \widetilde{H} = \{(e_N, e_H)\}$. □

Theorem 6 (Condición necesaria de la extensión)**.** Supongamos que G es una extensión de N sobre H. Entonces $G \cong N \rtimes_\phi H$, donde $\phi_H \to \mathrm{Aut}(N)$ es la acción conjugación.

Demostración. Como G es una extensión de N y H, entonces para todo $g \in G$, existen unos únicos $n \in N$ y $h \in H$ tales que $g = nh$. Construimos de esta manera la siguiente aplicación:

$$\begin{aligned} f : G &\to N \rtimes_\phi H \\ g &\mapsto (n, h). \end{aligned}$$

En primer lugar, está bien definida por la unicidad de n y h comentada previamente. Veamos que es un isomorfismo.

Para comprobar que es un homomorfismo, sean $g, g' \in G$. Entonces $g = nh$ y $g' = n'h'$. Por tanto,

$$\begin{aligned} f(gg') &= f(nhn'h') = f(nhn'h^{-1}hh') = (nhn'h^{-1}, hh') = \\ &= (n\phi_h(n'), hh') = (n,h) *_\phi (n',h') = f(g) *_\phi f(g'). \end{aligned}$$

Por otro lado, comprobar la biyección de f es sencillo. La aplicación f es claramente sobreyectiva. Ahora, sea $g \in \ker f$. Entonces $f(g) = f(nh) = (n,h) = (e,e)$, por lo que $g = nh = e$. Por lo que f es también biyectiva. $\square$

3. Escisión de secuencias cortas exactas

Definition 4. Una secuencia corta exacta de grupos $\{e\} \to N \xrightarrow{f} G \xrightarrow{g} H \to \{e\}$ **se escinde** si $\exists k : H \to G$ homomorfismo tal que $g \circ k = \mathrm{id}_H$.

Theorem 7. Sean G, H, N grupos. Son equivalentes:

1. $\{e\} \to N \xrightarrow{f} G \xrightarrow{g} H \to \{e\}$ es una secuencia corta que se escinde con $k : H \to G$.
2. $G \cong N \rtimes_\phi H$.

En este contexto, $\phi_h(n) = f^{-1}(k(h)f(n)k(h^{-1}))$.

Demostración. Demostremos la cadena de implicaciones en el orden establecido por el teorema.

(1⇒2) Notemos en primer lugar que $K(H), f(N) \leq G$. Tomemos el homomorfismo $k \circ g : G \to K(H)$. Por un lado, para todo $a \in K(H)$, tenemos que $a = k(h)$ para un cierto $h \in H$, por lo que $k(g(a)) = k(g(k(h))) = k(h) = a$, por lo que $k \circ g|_{K(H)} = \mathrm{id}_{K(H)}$. Por otro lado, $\ker(k \circ g) = \ker g = f(N)$ por ser una secuencia exacta corta. La primera igualdad viene del hecho de que $k(g(a)) = e$ si y solo si $g(a) = g(k(g(a))) = e$.

Por tanto, tenemos un homomorfismo de grupos $k \circ g : G \to K(H)$ que es la identidad en $K(H)$ y cuyo núcleo es $f(N)$. Por el teorema de extensión de grupos, G es una extensión de $f(N)$ sobre $k(H)$. De este modo, por el Teorema de la condición necesaria de extensión, $G \cong f(N) \rtimes_\varphi k(H)$, con $\varphi : k(H) \to \mathrm{Aut}(k(H))$ la acción por conjugación.

Además, f es inyetiva por la secuencia corta exacta, luego $f : N \cong f(N)$. Por otro lado, por el hecho de que la secuencia se escinde con $k : G \to H$, tenemos también que $k : H \cong k(H)$. Por el Teorema de Isomorfía, $f(N) \rtimes_\varphi k(H) \cong N \rtimes_\phi H$, donde $\phi := \widehat{f^{-1}} \circ \varphi \circ k$ la cual si desarrollamos, obtenemos lo siguiente:

$$\phi_h(n) = f^{-1}(\varphi_{k(h)}(f(n))) = f^{-1}(k(h)f(n)k(h^{-1})).$$

(2⇒1) Consideremos en primer lugar $G = N \rtimes_\phi H$ Por teorema, $f : N \to N \rtimes_\phi H$ tal que $f(n) = (n, e_H)$ es un isomorfismo. Además, definamos $g : N \rtimes_\phi \to H$ tal que $g(n,h) = h$. Entonces g es un homomorfismo sobreyectivo tal que $\ker g = N$. De este modo, podemos establecer la siguiente secuencia corta:

$$\{e\} \to N \xrightarrow{f} N \rtimes_\phi H \xrightarrow{g} H \to \{e\}.$$

Veamos que esta secuencia es exacta. En primer lugar, como f es inyectiva, $\ker f = \{e\}$. Por otro lado, por ser f sobreyectiva, $\mathrm{im}(f) = N = \ker g$. Finalmente, por ser g sobreyectivo, $\mathrm{im}(g) = H$. Esto demuestra que es una secuencia corta exacta. Veamos ahora que se escinde.

Tomemos la aplicación $k : H \to N \rtimes_\phi H$ tal que $k(h) = (e_N, h)$. Esta aplicación es claramente un homomorfismo y además, $g(k(h)) = g(e_N, h) = h$, luego esto demuestra que la secuencia exacta corta se escinde.

Finalmente, podemos obtener la expresión de ϕ en función de f y k como sigue:

$$f(\phi_h(n)) = (\phi_h(n), e_H) = (\phi_h(n), hh^{-1}) = (e_n, h) *_\phi (n, e_H) *_\phi (e_N, h^{-1}) = k(h)f(n)k(h^{-1}).$$

Para el caso general de $G \cong N \rtimes_\phi H$, tomando el isomorfismo dado $\psi : N \rtimes_\phi H \to G$ y los mismos homomorfismos f, g y k de los párrafos anteriores, basta considerar la secuencia $\{e\} \to N \xrightarrow{\psi \circ f} G \xrightarrow{g \circ \psi^{-1}} H \to \{e\}$ con el homomorfismo $\psi \circ k : H \to G$ y se comprueba de manera rutinaria que esta secuencia es exacta y se escinde, además de que ϕ se puede expresar en términos de $f \circ \psi$ y $\psi \circ k$ como indica el teorema. $\square$